WINTER 2022 / ISSUE NO.20

$ 15.00 | € 10.00 | 1500 RSD

HORIZONS

ISSN 2406-0402

JOURNAL OF INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

A CYBER ODYSSEY

QUANTUM OF HOPE

ÇIRAKLI • CORDERO • D'AGOSTINO • DORSEY • GUÉHENNO • HAASS
LANDAU • MARGULIES • ORESKES • PANNIER • RUBINSTEIN • SALEM ALDHAHERI
SEREN • SUCHKOV • ÜLGEN • UMAR • ZABIEREK • ZAKHEIM

cirsd.org

SUSTAINABLE DEVELOPMENT SOLUTIONS NETWORK

A GLOBAL INITIATIVE FOR THE UNITED NATIONS

Mobilizing global scientific and technological expertise to promote practical solutions for sustainable development.

The UN Sustainable Development Solutions Network (SDSN) has been operating since 2012 under the auspices of the UN Secretary-General. We support the implementation of the Sustainable Development Goals (SDGs) and the Paris Climate Agreement by accelerating joint learning and promoting integrated approaches.

Join the SDSN!

Over 800 universities, research institutes, and other knowledge-creating institutions are part of SDSN. Memberhship is free and entitles you to a wide-range of resources and networking opportunities. www.unsdsn.org/join

Learn With Us

The SDG Academy offers an ever-growing number of online courses on the SDGs, including agriculture and food systems, cities, early childhood development, resilience, and climate change. www.sdgacademy.org

Resources for the SDGs

The annual SDG Index and Dashboards report tracks country performance on the SDGs. Related products include regional SDG Indices, including for Africa, and city indices, including for the 100 largest cities in the USA. www.sdgindex.org

Join us for an upcoming event, such as the International Conference on Sustainable Development or the Low-Emissions Solutions Conference!

info@unsdsn.org
www.unsdsn.org
@unsdsn

McCANN
BEOGRAD

TruthWell Told

Every day we tell true stories about brands. And this too, is a true story. About us. Our youngest employee was born when our oldest employee started work. Our client is a company with over 10,000 employees. Our client is a company with one employee. In their free time our people are illustrators, screen writers, singers, writers, comic book illustrators, musicians, yoga instructors, sculptors, psychologists, journalists, travelers, photographers, economists, sociologists, filmmakers, consultants, translators. At work, our people are illustrators, screen writers, singers, writers, comic book illustrators, musicians, yoga instructors, sculptors, psychologists, journalists, travelers, photographers, economists, sociologists, filmmakers, consultants, translators.

Our people are **McCann Belgrade. McCann Belgrade** is our people.

www.mccann.rs

cirsd

Published by
Center for International Relations and Sustainable Development

EDITORIAL OFFICE: *Horizons*, Sredačka 10, Belgrade, 11000, Serbia. Telephone: +381-11-244-0465, Fax: +381-11-266-0764. Email: horizons@cirsd.org. Website: www.cirsd.org

SUBSCRIPTION OFFICE: Postmaster and subscribers please send address changes and subscription inquiries to: *Horizons*, Sredačka 10, Belgrade, 11000, Serbia. Telephone: +381-11-266-0760, Fax: +381-11-266-0764. Email: horizons@cirsd.org. Website: www.cirsd.org/horizons

Horizons is published by the Center for International Relations and Sustainable Development (CIRSD).

Cover design: McCann Beograd.

ЦИП - Каталогизација у публикацији
Народна библиотека Србије, Београд
327
HORIZONS
ISSN 2406-0402 = Horizons
COBISS.SR-ID 209682444

Horizons is printed by
Vizartis d.o.o.
Miloja Zakića 27
Belgrade, 11030, Serbia.
Telephone: +381-11-2317-771
+381-11-2317-876
Fax: +381-11-2317-873

Editorial

TODAY, it suffices to have a smartphone to instantly access a vast repository of human knowledge and conduct one's professional and even personal life with few impediments. Tomorrow, countries and corporations will require next-generation supercomputers to run their affairs. Obsolescence will be the fate of those failing to keep up, for the quantum computing age will have wrought a revolutionary transformation of much of what we know. The unplumbed effects will be felt in every corner of the planet.

SOMEWHERE in the rough and tumble of our contemporary technological achievements, what we assumed to be secure and private became radically altered. Across much of the world, citizens' conversations and movements are recorded as a matter of course. Social media algorithms peddle fake or manipulated news and pseudo-science for profit or influence, as various forms of cyber activity imperil the integrity of elections near and far.

HARDLY any of this is regulated at the global level—even close allies find it difficult to come to terms on governance frameworks to manage such platforms and technologies. Should the political will to take action somehow be found, the disorienting rapidity of the changes taking place are such that any binding treaty on these and similar subjects would be at least partly obsolete by the time it entered into force.

IN SHORT, humanity is on a cyber odyssey of accelerating velocity and unknown destination—the strategic, geopolitical, socio-economic, and moral implications of which are only beginning to be examined profoundly. We are thus fortunate indeed to feature in this edition of *Horizons* the views and recommendations of some of the world's most renowned authors on these weighty matters.

OF EQUAL renown are the contributors whose reflections and judgments we feature in the section entitled "Coming to Terms with Afghanistan." The world joined hands in solidarity with a superpower in its campaign to extinguish the terrorist organization that perpetrated an attack on its soil, together with those who granted its members safe harbor. Many of the partnerships thence established have since dissipated, as the clarity of America's reckoning got lost in the fog of multiple wars. The design and execution of the U.S. withdrawal from Afghanistan has caused much perturbation, even amongst its staunchest of allies—the latest manifestation of the disconcerting realities of our disorderly world.

UNDER such circumstances, a number of middle powers are acting more boldly upon their rising aspirations. One of these is Turkey, whose more exertive foreign policy was first made manifest in the wake of the launch of the War on Terror. Measured assessments of the results of Ankara's quest for autonomy on the international stage round out the milestone twentieth edition of our journal.

CONTRIBUTORS

MUSTAFA ÇIRAKLI is an Associate Professor of International Relations and Director of the Near East Institute at Near East University.

CARRIE CORDERO is Robert M. Gates Senior Fellow at the Center for a New American Security and was Counsel to the U.S. Assistant Attorney General for National Security and Senior Associate General Counsel to the Director of National Intelligence.

JOHN D'AGOSTINO is Senior Advisor to Coinbase and lectures on Fintech at Columbia University.

JAMES M. DORSEY is a Senior Fellow at the National University of Singapore's Middle East Institute.

JEAN-MARIE GUÉHENNO is Arnold A. Saltzman Professor of Practice in International and Public Affairs at Columbia University and was UN Under-Secretary-General for Peacekeeping Operations and President and CEO of the International Crisis Group.

RICHARD HAASS is President of the Council on Foreign Relations and was U.S. President George W. Bush's Coordinator for the Future of Afghanistan and Director of Policy Planning at the U.S. State Department.

CONTRIBUTORS

SUSAN LANDAU is Bridge Professor of Cyber Security and Policy at the Fletcher School and the School of Engineering of Tufts University and was Senior Staff Privacy Analyst at Google and Distinguished Engineer at Sun Microsystems.

PETER MARGULIES is Professor of Law at the Roger Williams University School of Law.

NAOMI ORESKES is Professor of the History of Science and Affiliated Professor of Earth and Planetary Sciences at Harvard University.

ALICE PANNIER heads the Geopolitics of Technology program at the French Institute of International Relations (IFRI).

IRA RUBINSTEIN is a Senior Fellow at the Information Law Institute of the New York University School of Law and was Associate General Counsel in charge of the Regulatory Affairs and Public Policy group at Microsoft.

MOHAMED JOUAN SALEM ALDHAHERI is Executive Chairman, CEO, and Co-founder of RainMKRS.

CONTRIBUTORS

MERVE SEREN
is an Assistant Professor in Political Science at Ankara Yıldırım Beyazıt University and a former Parliamentary Advisor to the Grand National Assembly of Turkey.

MAXIM A. SUCHKOV
is Acting Director of the Institute of International Studies and an Associate Professor at MGIMO University and an expert affiliate of both the Valdai Discussion Club and the Russian International Affairs Council (RIAC).

SINAN ÜLGEN
is a Visiting Scholar at Carnegie Europe and Executive Chairman of EDAM.

SÜHA UMAR
is a retired Ambassador of the Republic of Turkey who served in that capacity in Jordan and Serbia and was also Director General for Bilateral Political Affairs of the Foreign Ministry of the Republic of Turkey.

LAUREN ZABIEREK
is Executive Director of the Cyber Security Project at the Belfer Center of the Harvard Kennedy School of Government and was formerly a U.S. intelligence analyst.

DOV S. ZAKHEIM
is a Senior Adviser at the Center for Strategic and International Studies and was U.S. President George W. Bush's Under Secretary of Defense and U.S. President Ronald Reagan's Deputy Under Secretary of Defense.

Table of Contents

WINTER 2022 / ISSUE NO. 20

HORIZONS

Table of Contents

WINTER 2022 / ISSUE NO. 20

How Cybersecurity Saved U.S. Democracy

Carrie Cordero

ACCORDING to a 12 November 2020 joint statement of U.S. election officials, the 2020 U.S. presidential election "was the most secure in American history." That success was a result not of accident, but instead of deliberate, sustained, and comprehensive efforts at the local, state, and federal levels to ensure that it was secure from foreign interference. Those efforts to secure the election were borne out of the attempts by the Russian government to influence the outcome of the 2016 U.S. presidential election. In the end, however, the efforts to enhance the cybersecurity of the U.S. electoral infrastructure in 2020 ended up protecting the integrity of the election not only from malign foreign activities, but also from domestic anti-democratic and illiberal efforts to undermine confidence in the 2020 presidential election.

A range of activities designed to protect the American election infrastructure from foreign malign activity ended up providing a bulwark against threatening domestic efforts to undermine and overturn the lawful election result. The U.S. experience in 2020 suggests that cybersecurity itself can play a critical role in protecting not only election infrastructure as a technical matter, but also providing a technical basis to counter illiberal forces as a mechanism to protect the democratic process of conducting a fair election. Cybersecurity itself just may have saved U.S. democracy from careening of the rails, continued sustained efforts to continue to harden election infrastructure cybersecurity and create a cadre of trusted officials, will likely be needed again.

Carrie Cordero *is the Robert M. Gates Senior Fellow and General Counsel at the Center for a New American Security, Adjunct Professor at Georgetown Law, and a CNN legal and national security analyst. She previously served as Director of National Security Studies at Georgetown Law, Counsel to the U.S. Assistant Attorney General for National Security; Senior Associate General Counsel at the Office of the U.S. Director of National Intelligence; and Attorney Advisor at the U.S. Department of Justice. This essay draws, in part, from materials produced as part of the CNAS commentary series on Bolstering American Democracy Against Threats to the 2020 Elections, as well as congressional testimony by the author on foreign interference in the U.S. 2016 election, in June 2019. You may follow her on Twitter @carriecordero.*

Photo: Guliver Image/Getty Images

On 6 January 2021 a mob stormed the U.S. Capitol, delaying the election's certification

Despite the success of U.S. cybersecurity and intelligence activities in protecting against malign foreign influence, the voting mechanisms and outcome of the 2020 American election has been subject to persistent allegations of fraud and inauthenticity by malicious domestic partisans. These domestic political actors seek to lower voter confidence in the outcome, thereby politically damaging their opponents and undermining confidence in future elections that they lose. As of this writing former President of the United States Donald Trump has not publicly accepted the validity of the 2020 election outcome, and a significant percentage of Americans identifying as Republicans still did not believe that President Joe Biden had lawfully won the 2020 election.

When the U.S. Congress reconvened after the insurrection that delayed the certification of the vote on 6 January 2021, 147 Republicans voted to sustain the false challenges to the vote outcomes in Arizona and/or Pennsylvania. And yet, despite the political support from Republican politicians and their supporters between 3 November 2020 and 6 January 2021 to re-engineer the outcome of the election, these pernicious efforts were largely able to be

credibly rebuffed and refuted This ability to confirm the election outcome was a significant downstream effect of the engagement of the cybersecurity community and activities that had been implemented across the country leading up to the 2020 presidential election.

The effective functioning of American democracy is being strained by the recent unravelling of the U.S. social and political construct that lawfully-conducted election outcomes are respected and accepted by both the winning and losing candidates. That being said, the experience and challenges presented by the U.S. 2020 election and accompanying improvements that were made to secure the election from a cybersecurity perspective provided necessary assurances that the election outcome was accurate and fair. This experience provides lessons not only for the U.S., but for the international community interested in ensuring that elections are not only free from both technical cyber intrusion by malign foreign actors, but also fortified against countering disinformation about the security of the election architecture itself.

The U.S. experience in 2020 suggests that cybersecurity itself can play a critical role in protecting not only election infrastructure as a technical matter, but also providing a technical basis to counter illiberal forces as a mechanism to protect the democratic process of conducting a fair election.

The lesson that can be drawn from the U.S. experience in the 2020 presidential election is that accurate technical data and expertise is the best defense to refute international or domestic misinformation and malice to undermine democratic elections. In other words, cybersecurity—and the expertise and credibility of those in charge of it—is turning out to be the best defense against efforts to undermine democratic elections. Security of election administration is paramount for securing democracies and protecting against foreign or domestic efforts to undermine the actual outcome or confidence in the outcome.

How to Endanger an Election

We know the story of the 2016 U.S. presidential election: malign foreign cyber activity directed by the Russian government and its surrogates was conducted against the U.S. population and election ecosystem. The Russian efforts to influence the election were substantially documented in two independent investigations. The first, completed in March 2019 but not released by former Attorney General Bill Barr until 18 April 2019 (and then only in redacted form), was Volume I of the *Report on the Investigation Into Russian Interference in the 2016 Presidential Election*, as a result of the investigation led by Special Counsel Robert S. Mueller III, a former FBI director. The Special Counsel's investigation exposed a sustained, systematic intelligence operation by the government of Russia to interfere in the 2016 election.

According to the Special Counsel's report—and as I described in June 2019 during my testimony before the U.S. House Committee on the Judiciary—the Russian activities started as an information warfare operation intended to affect the election generally, and by 2016 was actively working to help Trump win. According to the report, the operation involved two main efforts. The *first* was a social media operation intended to influence Americans' public opinion. The effort was successful in reaching millions of Americans through social media engagement, false online personas, and ad buys. The *second* part of the influence campaign involved computer hacking to steal and then release information from the Democratic campaign apparatus, including the Hillary Clinton campaign, the Democratic National Committee, the Democratic Congressional Campaign Committee, and the emails of her campaign chairman John Podesta.

The lesson that can be drawn from the U.S. experience in the 2020 presidential election is that accurate technical data and expertise is the best defense to refute international or domestic misinformation and malice to undermine democratic elections.

In addition, as I also discussed in my June 2019 for-the-record statement, there was arguably a *third* component, which the report discusses as part of the social media operation. This component often gets overlooked: Russian operatives caused real, unsuspecting Americans to organize rallies and gather for political purposes. These foreign operatives pretended to be American grass roots activists. These online operatives made contact and interacted with Trump supporters and Trump campaign officials.

Trump campaign officials amplified social media posts produced by the Russian Internet Research Agency (IRA). Individuals influenced by Russian activities organized real-world rallies. As I wrote in my 2019 for-the-record statement, the 2016 activities were a combination of social media engagement, criminal cyber intrusion, and political organization on the ground in local American communities.

The second comprehensive, independent investigation was the five-volume report issued by the Senate

Select Committee on Intelligence, which documented the active measures and social media influence effectuated by the Russian government and its surrogates, American intelligence assessments, the U.S. response to these activities, and the counterintelligence threats and vulnerabilities reviewed by the committee.

Taken together, these collective reports comprising thousands of pages issued by components of two separate branches of the U.S. government established a compelling narrative explaining Russian efforts to influence the U.S. election through direct malign cyber activity, social media information operations, and other attempts to influence U.S. public opinion in the physical world.

In 2020, not only was the Russian government engaged in varying levels of attempted influence on the election outcome, but also Iranian and Chinese government actors.

How to Protect an Election

In 2020, the threats compounded as compared to 2016. Not only were there Russian government efforts—although not on the scale of the 2016 influence campaign—but according to the U.S. intelligence community, Iranian and Chinese government actors also engaged in varying levels of attempted influence on the 2020 election outcome.

Moreover, as election day passed, the greatest threat to public confidence in the election outcome came from domestic politics: Trump and his political allies led an aggressive campaign to undermine confidence in the election and try to overturn the election outcome. This effort came to a head in the events of 6 January 2021 when a mob stormed the U.S. Capitol, causing the delay of the certification of the election by the U.S. Congress. Five people died, including U.S. Capitol Police Officer Brian Sicknick.

The improved set of efforts in 2020 by the United States were the result of three main lines of effort: a whole of government initiative, which involved activities at the federal, state, and local levels; technical defenses, which were bolstered by U.S. federal resources and expertise offered; and credible messengers, including senior level American national security and cybersecurity leaders who were willing to provide accurate information in public, regardless of the professional consequences, including, in some cases, political retribution and threats to their own personal safety and that of their families. Each of these components provided a basis upon which the independent U.S. media could accurately report and amplify accurate information regarding the reliability of voting systems, and the legitimacy of the 2020 election outcome.

As Erik Brattberg of the Carnegie Endowment for International Peace explained in a commentary that was part of a series on foreign interference published by the Center for a New American Security (CNAS), America was not alone in 2020 in working to secure elections against foreign influence efforts: "Russia's interference in the November 2016 U.S. presidential election served as a wake-up call for Europe about the rising threats facing free and fair elections." Brattberg outlined how efforts in EU member states to elevate election security as a priority national security issue, assist political parties and campaigns with cybersecurity expertise and resources, and focus on voter education all contributed to building more resilient elections in various European Union member states.

The effort to protect the actual security of the 2020 election and counter post facto allegations that it was unsecure required a whole of nation effort.

Coordinating Government Entities.

American elections are run locally; the U.S. federal government does not administer them and is not in charge of them. The effort to protect the actual security of the 2020 election and counter post facto allegations that it was unsecure required a whole of nation effort that ranged from the Cybersecurity Infrastructure Security Agency (CISA) of the Department of Homeland Security and other parts of the intelligence community to state and local election officials, but also included a range of private sector entities that facilitated the implementation of technical defenses.

As a result of what happened in 2016, local, state, and federal officials took far greater steps over the subsequent four years to ensure that there would not be a repeat performance in 2020. As Deputy Secretary of State for the State of Connecticut Scott Bates wrote as part of the aforementioned series on foreign interference published by CNAS, "the challenge for us as a nation is that it is not the federal government that runs our election system, but that responsibility resides with the 50 states. Thus, it's up to each of the 50 states to defend itself against aggressive nation-states." According to Bates, Connecticut implemented a plan leading up to the 2020 election that, *one*, provided National Guard resources so that assessments of individual municipalities' cybersecurity readiness could be undertaken; *two*, provided and state resources to update computer systems; *three*, supported election cybersecurity education and training, and *four*, put a communications plan in place to counter disinformation.

The U.S. federal government had a meaningful role to play in providing expertise and resources before the

election. Leading up to the 2018 midterm elections and continuing through the 2020 campaign season, CISA prioritized election security at the top of its agenda. As former CISA Director Chris Krebs wrote in the same aforementioned CNAS series, the designation of the election systems as "critical infrastructure" was integral to acknowledging that "election infrastructure is of such vital importance to the American way of life that is incapacitation or destruction would have a devastating effect on the country."

CISA was able to convene state and local election officials alongside private sector partners to foster a robust election security community and facilitate the sharing of technical expertise and resources.

In fact, CISA was able to convene state and local election officials alongside private sector partners to foster a robust election security community and facilitate the sharing of technical expertise and resources. As described below, CISA's activities in marshalling the lessons and insights from its work to improve technical defenses proved integral in using its communications capabilities to authoritatively refute baseless allegations of voter fraud and voting machine malfunction and exploitation.

Hardening Technical Defenses.

The decentralization of the U.S. election infrastructure turns out to be an advantage; centralization increases risk. The private sector served a pivotal role in working with government officials to implement cybersecurity initiatives. Some private companies worked to provide cybersecurity related services and resources free of cost to political campaigns and state and local websites. State and local governments, however, often short on resources, had varying levels of modernized hardware and software supporting election administration. The federal government was able to effectively provide technical expertise to states and localities, and coordinate efforts across the country.

Here's how Krebs described CISA's efforts to improve the technical security of the decentralized U.S. election infrastructure:

> For both in-person and mail-in voting, we are helping election officials secure the underlying systems and processes by providing a range of services, such as system vulnerability scans on a weekly basis, remote penetration testing for hundreds of jurisdictions and dozens of states, and phishing assessments. There is no question the security posture of election systems is getting better. We have observed improved patch rates, increased adoption of multifactor authentication, more regular backups, and expanded logging of systems, to name just a few. We have worked with the largest election technology providers in the country to pick their systems apart, looking for vulnerabilities, and helped them mitigate those vulnerabilities. We continually work to map out and understand the various systems, mechanisms, processes, and techniques used across the election community to determine where the riskiest bits are and what is effective at managing those risks. One of the best risk management and resilience-building techniques we have found is paper. We continue to encourage states to shift to systems with a paper record associated with every vote—which is essential, because of the ability to audit such records. In 2016, 82 percent of votes cast were associated with a paper record, and for 2020 we project more than 92 percent of votes cast will have a paper record.

Importantly, the range of technical defenses includes the least technological but a critical aspect of providing a verifiable result: paper ballot backups. From 2016 to 2020, the percentage of states with paper ballot backups significantly increased, not all states had paper ballot backups available for all voters in 2020. The existence of paper ballot backups is something that all election administrators should work to facilitate, as the availability of the backup can facilitate an actual recount, if needed, as well as a bulwark against allegations that machines are at fault and cannot be verified.

Amplifying Credible Messengers

The presence of cybersecurity activities provided credible government officials with a basis upon which to offer accurate information to the public, but also to be believed. The assurances by public officials were not just empty assurances that election results could be trusted—they were assurances based on the facts of how elections are verified through extensive processes, and on the enhanced understanding and attention that state and local officials had dedicated to improving the cybersecurity of the election technology infrastructure since 2016. In addition, the credibility of the message was enhanced when the messengers themselves ranged from unelected national security leaders to elected and partisan state election officials.

At the U.S. federal level, senior national officials, including FBI Director Chris Wray, National Counterintelligence Executive William Evanina, and CISA Director Chris Krebs provided the public with non-partisan, unclassified information regarding the nature of the foreign threats to the 2020 election. As the election drew near, these leaders released video messages outlining the threat posed by foreign adversaries and communicating the

✓ **Reality:** A compromise of a state or local government system does not necessarily mean election infrastructure or integrity of your vote has been compromised.

✕ **Rumor:** If state or local jurisdiction information technology (IT) has been compromised, the election results cannot be trusted.

Get the Facts: Hacks of state and local IT systems should not be minimized; however, a compromise of state or local IT systems does not mean those systems are election-related. Even if an election-related system is compromised, a compromise of a system does not necessarily mean the integrity of the votes has been affected. Election officials have multiple safeguards and contingencies in place, including provisional ballots or backup paper poll books that limit the impact from a cyber incident with minimal disruption to voting. Additionally, having an auditable paper record ensures that the vote count can be verified and validated.

Useful Sources
- FBI-CISA Public Services Announcement: Cyber Threats to Voting Processes Could Slow But Not Prevent Voting
- Election Infrastructure Cyber Risk Assessment, CISA
- Link directly to this rumor by using: www.cisa.gov/rumorcontrol#rumor5

Example A

national security community's attention to preventing foreign interference from Russia, Iran, and China from successfully impacting the election.

In 2020, CISA created a webpage entitled Rumor Control as part of its public communications strategy to counter disinformation originating from malign foreign activity directed against the upcoming November 2020 presidential election. This website was integral to these efforts to combat misinformation—whether foreign or domestic in origin.

There, on a rolling basis, CISA posted accurate, verified information dispelling myths and other inaccurate information about the election, shooting down myths that were arising with increasing frequency as the election neared with real-time information about how voting systems actually work (see Example A).

But Rumor Control became even more important in the days after the election, using its expertise, credibility, and platform to counter domestic efforts from the incumbent president, his political surrogates, and political allies in certain key states where the vote count was close (see Example B).

Krebs shared the information that was published on CISA's Rumor Control website on his personal Twitter account and used his own professional credibility as a cybersecurity professional willing to work across party lines to counter the post-election attacks on the credibility of the election outcome.

✓ **Reality:** Robust safeguards including canvassing and auditing procedures help ensure the accuracy of official election results.

✕ **Rumor:** A bad actor could change election results without detection.

Get the Facts: The system and processes used by election officials to tabulate votes and certify officials results are protected by various safeguards that help ensure the accuracy of election results. These safeguards include measures that help ensure tabulation system function as intended, protect against malicious software, and enable the identification and correction of any irregularities.

Every state has voting system safeguards to ensure each ballot cast in the election can be correctly counted. State procedures often include testing and certification of voting systems, required auditable logs, and software checks, such as logic and accuracy tests, to ensure ballots are properly counted before election results are made official. With these security measures, election officials can check to determine that devices are running the certified software and functioning properly.

Every state also has laws and processes to verify vote tallies before results are officially certified. State processes include robust chain-of-custody procedures, auditable logs, and canvass processes. The cast majority of votes cast in this election will be cast on paper ballots or using machines that produce a paper audit trail, which allow for tabulation audits to be conducted from paper record in the event any issues emerge with the voting system software, audit logs, or tabulation. These canvass and certification procedures are also generally conducted in the public eye, as political party representatives and other observers are typically allowed to be present, to add an additional layer of verification. This means voting system software is not a single point of failure and such system are subject to multiple audits to ensure accuracy and reliability. For example, some countries conduct multiple audits, including a post-election logic and accuracy test of the voting system, and bipartisan hand count of paper ballots.

Example B

On 12 November 2020, CISA published a joint statement from the Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Council Executive Committees confirming the integrity of the election mechanics and refuting allegations of voting machine manipulation or error. On 17 November 2020, Trump fired Krebs, who was the subject of threats of violence for his efforts to publicly refute false election narratives.

State leaders, particularly Republicans who refused to go along with the false allegations of voter fraud and election machine malfunctions, also served a critical role in combatting domestic political disinformation about the election outcome.

For example, the fact that Georgia Secretary of State Brad Raffensberger was an elected Republican who publicly countered the false election fraud narrative added to his credibility that the election outcome in Georgia could be trusted. Raffensberger and other Georgia election officials spoke out publicly against Trump's false public accusations of voter fraud as well as private pressure he directed at them in phone calls—all at the

risk of what became persistent threats to their safety and that of their families. The Raffensberger family continued to receive death threats for the Georgia Secretary of State's role in upholding the credibility of the election outcome for many months after the election and even after the presidential inauguration of Joe Biden.

The 2016 activities were a combination of social media engagement, criminal cyber intrusion, and political organization on the ground in local American communities.

The U.S. Justice Department launched a task force intended to investigate and prosecute threats against election officials as threats increased—whether directed against elected officials, political appointees, non-partisan poll workers, or other election officials at state and local levels. As recently as late October 2021, the Florida Supervisors of Elections, currently with a Republican majority, issued a letter pleading with political candidates to "tone down the rhetoric and stand up for our democracy" in the face of "disinformation, misinformation, and malinformation" that has led to threats directed against election officials and undermines confidence in democratic institutions.

Cybersecurity's Continued Role

Election integrity measures do not only involve the technical aspects of administering elections. In addition to securing the technological aspects of election administration, bureaucratic and administrative processes that take place after votes are cast are functions that provide voter confidence in the result. As Matthew Weil and Christopher Thomas of the Bipartisan Policy Center explained in an October 2021 paper on election integrity, a variety of "security and integrity measures" are currently in place at the state and local levels in order to provide redundancy and accuracy of election outcomes. These include but are not limited to establishing a proper chain of custody, records of tabulations, and audit trails. Ensuring an election in which citizens have confidence involves not only actually securing the election technology and mechanics, but being able to provide transparency about the process and rules that are followed.

In the U.S., threats to elections are multifaceted. Over the long term, the success of the Russian 2016 influence and intrusion campaign provides foreign adversaries with substantial evidence that the investment can be low, but the reward can be high for engaging in activities intended to affect not just American elections but the fabric of U.S. society itself. According to the U.S. intelligence community, Russia and Iran tried their hand at more limited acts of interference in 2020. It would not be surprising if these or other countries with interests of their own targeted U.S. elections in the future with either malign cyber intrusion activity or perhaps a more pernicious social media influence. Thus, the U.S. national security and intelligence components will need to continue to be vigilant about identifying and countering malign foreign influence on future elections.

The U.S. political environment is so damaged that disinformation about the integrity of the election infrastructure will remain a persistent part of the national political conversation.

At least in the short term, however, the U.S. political environment is so damaged that disinformation about the integrity of the election infrastructure will remain a persistent part of the national political conversation. Even in an off-year election, for example, the Republican candidate for Governor of Virginia that took place in early November 2021 (he ended up winning) made "election integrity" a centerpiece of his campaign, with calls to audit Virginia's voting machines, despite no credible facts that Virginia's voting systems are unsecure. This current and unfortunate political environment places cybersecurity and other national security officials—who would generally prefer to avoid engaging in dialogue concerning the election for fear of being perceived as partisan—squarely with the responsibility of countering damaging allegations of vote tampering, equipment malfunctions, and other fabricated statements about the election infrastructure.

In the future, cybersecurity officials at the federal, state, and local levels will be able to look at the 2020 election as an example of how—in the face of persistent efforts to paint voting infrastructure as insecure—the work that went into securing the election ecosystem provided a factual, credible basis upon which to effectively counter malign domestic forces intent on undermining and overturning the election. Continued engagement of cybersecurity experts who work to coordinate government entities, harden technical defenses, and bolster those that are credible messengers will provide an invaluable service to the country by not only securing elections, but protecting democracy.

THE CONFLICT OVER CRYPTOGRAPHY

BATTLING OVER DIFFERING VERSIONS OF SECURITY

Susan Landau

REVOLUTIONS are messy things, and the Digital Revolution is no exception. It has created new opportunities and new risks, new centers of power, and, in a truly revolutionary style, serious new threats that allow attackers from half a world away to threaten—and sometimes cause—serious damage without physically crossing a border. It has also allowed new types of crime to flourish.

Some regimes—including Russia, China, and Iran—that seek information security as well as cybersecurity are building their own internets in order to limit access to the rest of the world and restrict the ability of information to transit borders. Other nations, supporting the free flow of information, want cybersecurity—in contradistinction to what is called information security. They are struggling to prevent cyber exploits (theft of data), cybercrime, and cyberattacks from within and outside their borders. Here is where the conflict about cryptography arises.

Cryptography secures communications and protects data at rest—but that very same technology can also complicate, and even prevent, criminal investigations. It can hide the tracks of spies. For years the battle over the public's use of strong encryption technology has been described as a battle over privacy versus security. But that description misses how our society has changed and how reliance on ubiquitous, easy-to-use cryptographic systems—iMessage, Signal, automatic secure locking of smartphones, and so on—are necessary not just for individual privacy but to provide security. Widespread use of cryptography enhances national security, public safety,

Susan Landau *is Bridge Professor of Cyber Security and Policy, The Fletcher School and School of Engineering, Tufts University. She was previously a senior staff privacy analyst at Google and held the post of Distinguished Engineer at Sun Microsystems.*

Photo: Photo Stock

security from hostile foreign actors—and, yes, privacy. The cryptography debate is really a debate about security versus security. And that makes it very complicated.

Battles over the public use of strong encryption systems started in the 1970s, when public-key cryptography first made its appearance. A cryptosystem has two parts: the algorithm, or method of encryption, and the key that is used with it. Here we can give the well-known Caesar shift system as an example. In this system, each letter is shifted—an "a" in the unencrypted version becomes a "D," a "b" becomes an "E," etc.—where "shifting" would be considered the algorithm, while "3" would be considered the key, since each letter is shifted three letters. A more interesting encryption system is a substitution cipher, in which the letters are randomly mixed: an "a" might become a "T," a "b" an "F," and so on. In this case, the algorithm is the substitution, and the key is the table that reveals that an "a" becomes a "T."

Since the late 1800s, the basic tenet of cryptography has been that the encryption algorithm should be public—many eyes viewing it can help ensure that the method is actually secure—but that the

encryption keys should be kept private to the people who are actually communicating. That made the issue of "key exchange" complicated because security dictates that keys should be frequently changed. Otherwise, it becomes easier for an adversary to discern patterns and thus decrypt captured messages.

Bedevilments and Battles

Key exchanges bedeviled cryptographers. It is one thing when two people can agree on an algorithm and exchange keys in person before they need to communicate confidentially, but quite another if they run out of keys. This happened to the USSR during the Second World War, when it could not supply its embassies with fresh cryptographic keys. Its diplomatic representations reused keys, which allowed the National Security Agency (NSA) to later decrypt communications they had collected from encrypted Soviet transmissions sent during the war.

With the arrival of the internet, it was not just diplomats and spies that needed secret key exchanges—everyone did.

With the arrival of the internet, it was not just diplomats and spies that needed secret key exchanges—everyone did. For example, when you choose to buy something from a website, you need to protect the credit-card number you submit. But how do you do that if it's the first time you have ever been to that website? Public-key cryptography, which is based on problems that are fast to compute but much slower to reverse, provides the mathematical magic enabling secure key exchange. When Stanford and MIT computer scientists developed the idea in the mid 1970s, the national-security community pushed back; they had been the ones doing cryptographic research, not university professors or industry researchers, and they expected to continue to own it.

Thus began many decades of battles over the public's use of strong cryptography—cryptography hard to undo except by trying all possible keys (a so-called "brute force" attack). The NSA first tried to prevent publication of research in cryptography, then it sought to control government development of cryptographic standards, and finally in the 1990s, it used export controls to slow the deployment of cryptographic systems. Such control also slowed the use of strong cryptographic systems within the United States, a result that had strong FBI support. Because the European Union had similar export controls, it was difficult for the public to obtain communication or computer systems with strong cryptographic capabilities.

Then, in the late 1990s, the situation changed. American industry had been pressing the U.S. Congress to lift the imposed controls. Meanwhile, the NSA was discovering that it was not just technologically-sophisticated countries that were deploying strong cryptography; many less technically sophisticated states were as well. The NSA needed to move to other methods, namely Computer Network Exploitation (CNE), to gain access to other nations' information. Basically, the NSA made a deal with Congress: it would not oppose a change in the regulations that would allow American companies to export systems with strong cryptography so long as the systems were not custom-made or sold to governments or telecommunications providers. In exchange, the NSA would receive government support to increase its CNE capabilities (the NSA's success in the latter is clear from the Edward Snowden disclosures). The EU, informed of the intended U.S. policy change, similarly loosened its export control requirements on cryptographic equipment, slightly prior to the U.S. modification. The FBI was not happy about this change, fearing that its ability to wiretap would quickly disappear. That did not occur, at least not immediately. In fact, at that time mobile phone providers did not even encrypt the radio transmissions between a mobile phone and cell tower.

With the change in cryptography controls, many computer scientists expected an avalanche of tools enabling end-to-end encrypted (E2EE) communications.

With the change in cryptography controls, many computer scientists expected an avalanche of tools enabling end-to-end encrypted (E2EE) communications (encrypted from the user to the receiver, thus preventing an interceptor from reading the message). Developed in the 1990s, PGP encryption could do so, but its architecture and interface presented barriers for the technology to become widely used by consumers. Instead, the first mass use of encryption turned out to be in securing phones.

Mobile Phones Lead the Way

Apple launched the iPhone—both a phone and a computer—in 2006. The phone became popular quickly, especially after Facebook became available to the public in 2007. The phone also caught on quickly with thieves, who found the small, expensive device easy to steal and resell. Apple countered by developing a feature called Find My iPhone, which caused theft rates to drop (Android's equivalent, developed later, is Find My Device). But in the late 2000s, criminals had a new wrinkle: stealing data off lost and stolen devices, then using the information for identity theft. Securing the data on the phone became quite important.

Currently, out of the five U.S. companies that hold a dominant role in the Internet economy—Facebook, Amazon, Apple, Microsoft, and Google—Apple stands out because it is a hardware company. While Apple produces great software, the company's profits come from selling hardware: iPhones, iPads, iMacs, and the like. This implies that Apple looks at customers differently than Microsoft, which focuses on selling software, as well as Facebook, Amazon, and Google, which focus on selling whatever their advertising networks convince the consumer to buy.

Apple sought to move into the corporate marketplace, and that meant emphasizing security; the company wanted its devices to be fully private, which is also a form of security.

To a company that focused on selling hardware, such tracking of users was not particularly useful. Indeed, it was actually counterproductive. Apple sought to move into the corporate marketplace, and that meant emphasizing security. Corporate security included wiping data if phones were lost or stolen. Apple's vision went further; the company wanted its devices to be fully private, with only the user able to access information on them. Such privacy is also a form of security.

In 2008, Apple began working towards a system in which only the legitimate user could open the phone and access its data. This solution would prevent criminals from pulling personal and business data from lost or stolen phones. With the 2014 release of iOS 8, one would need the user's PIN to unlock around 90 to 95 percent of the phone's data (Apple could, of course, access data that the user stored in the iCloud). With the 2015 release of iOS 9, Apple made it much harder for anyone but the user to access data on the phone; the company designed the phone to erase its data after ten incorrect tries of the user PIN.

Though these protections increased security—and thus prevented certain types of crimes—they did not please law enforcement. FBI Director James Comey began giving speeches objecting strongly to Apple's security enhancement.

The conflict between Apple and the FBI over secure phones came to a head in 2016. Two terrorists had attacked a San Bernardino Health Department holiday party; the terrorists themselves were killed in a police shootout a few hours later. The terrorists had destroyed their personal phones and computers but left behind a locked work iPhone secured through the iOS protections. Law enforcement wanted the device opened.

The FBI argued the phone might contain critical data about the dead terrorist's contacts and sought Apple's help to counter the security protections built into the operating system in order to access this information. Apple replied that it was not under a legal obligation to do such extensive rewriting of its system and that, furthermore, there was a serious risk that developing such software would create undue security risks for all its phones. When the company refused to comply, the government took Apple to court. The case was mooted after an FBI consultant found a way around Apple's protections and unlocked the device.

The real issue was law enforcement seeking so-called "exceptional access"—access for law enforcement under court order—to secured mobile phones.

The FBI found no evidence on the phone, but that was not the real point of the battle. The real issue was law enforcement seeking so-called "exceptional access"—access for law enforcement under court order—to secured mobile phones. Ever since the change in export control laws, the FBI had been seeking ways to limit the domestic use of encryption. Arguing that law enforcement was "going dark" due to encryption preventing eavesdropping on wiretapped communications, the FBI sought relief through legislation or the courts. Now the FBI added the category of secured phones to the issue. Law enforcement outside the U.S. echoed the FBI's complaint. Some—but not all—national-security agencies added their voices to this as well.

There were also some striking opponents to the FBI's push for exceptional access. This included Former NSA Director Mike McConnell, former Secretary of the Department of Homeland Security Michael Chertoff, and former Deputy Secretary of Defense William Lynn III, who wrote in a *Washington Post* oped that "we believe the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server, and enterprise level without building in means for government monitoring." Another former NSA Director, Michael Hayden, told an interviewer that "we are probably better served by not punching any holes into a strong encryption system—even well-guarded ones." This viewpoint was echoed outside the United States, as well. Robert Hannigan, former director of the UK's Government Communication Headquarters said at a meeting at MIT: "I am not in favor of banning encryption. Nor am I my asking for mandatory 'back doors.'"

From Escrow to Exceptional Access

The fight over access to end-to-end encryption emerged in the 1990s. In 1993, the U.S. government proposed "Clipper," a system for encrypting digitized voice communications where the encryption keys would be split and stored with agencies of the U.S. federal government. This proposal garnered

support neither from foreign nations nor from American industry or private citizens.

Many objected to the fact that storing encryption keys with U.S. government agencies eliminated communications privacy despite the legal protections that the government pledged to include in the system. Others raised security objections. End-to-end encryption systems are designed to prevent intrusion, while the proposed escrow system would be at risk of compromise by those running the system. A more serious concern was that concentrating encryption keys in storage systems provides a rich target for attackers. Finally, escrow systems destroy "forward secrecy," in which keys are used for a single communication, then destroyed at the end of the communication. Such systems increase security while lowering costs, since the keys are needed only during the communication and are not stored afterwards. If communications are protected using forward secrecy, an attacker who gains access to keys will be able to decrypt data from that time until the breach is discovered and patched. The attacker would not be able to decrypt any previous communications because those keys were destroyed after use. Escrowing keys changes that calculus, increasing risk.

Widespread use of cryptography enhances national security, public safety, security from hostile foreign actors—and, yes, privacy. The cryptography debate is really a debate about security versus security. And that makes it very complicated.

The Clipper system did not catch on, and the U.S. government abandoned the idea in the late 1990s, shortly before the change in export controls. However, the FBI and U.S. law enforcement did not give up on the idea of accessing encrypted communications. They began to push for something called exceptional access instead.

Unlike escrowed encryption, exceptional access is not a specified technology. Instead, it is the belief that encryption systems could be designed to be secure yet enable legally authorized surveillance. Such an expectation flies in the face of what computer security experts have learned in over 50 years of designing secure systems.

The biggest problem stems from the complexity that an exceptional access system introduces. Such systems would be far more complex than the E2EE systems in use today and—as engineers know—this increases the risk of vulnerabilities. Furthermore, there is the issue of jurisdiction. In the case of the Clipper system, the issue presented itself as the proposal's inability to handle differing rules for differing jurisdictions. Which laws and whose access would apply in a trans-border phone call, for example?

Implementing exceptional access for a mobile phone bought in one country, used in a second to make a call to a third, is enormously complicated. Would there be a single regulatory environment? Would there be multiple ones? Such questions would need to be answered before an exceptional access system could possibly be implemented.

The NSA spying revelations created a breach between the U.S. technology companies and the government that lasted several years.

In addition to those problems with exceptional access systems, there were also other issues. Requiring exceptional access would mean eliminating forward secrecy, which immediately decreases security. Exceptional access would also put an end to "authenticated encryption," a technology that securely combines authentication (ensuring that the message has not been tampered with during transit) and confidentiality (ensuring the privacy of the communication). In the 1990s the two functions were done separately; combining them helped eliminate errors that caused vulnerabilities. But exceptional access would necessarily separate the two functionalities.

Snowden and Spyware

The 2013 Snowden disclosures, with their revelations of the vast collection and capabilities of the NSA, silenced U.S. law enforcement for several years. The issue was not in responding to court orders for customer content; the companies had done so, of course. Snowden revealed that U.S. technology companies had been targets of bulk collection, with the NSA siphoning data "wholesale" from tech company overseas data centers. Google, Yahoo, and Microsoft doubled down on securing their intra-company communications, and the public too began to think more about securing their own. The NSA spying revelations created a breach between the U.S. technology companies and the government that lasted several years.

In 2015 the Obama administration considered the law-enforcement arguments—and opted not to propose legislation on encryption. The rationale behind the decision included benefits to civil liberties and human rights, a potentially positive effect on U.S. economic competitiveness, and increased security through broader use of encryption, even while acknowledging that such broader use could potentially impede law enforcement efforts. One sentence in a draft options paper for the U.S. National Security Council paper was particularly striking,

"[B]ecause any new access to encrypted data increases risk, eschewing mandated technical changes ensures the greatest technical security." In other words, American national security interests are best protected through the broader use of encryption throughout the infrastructure—and that is best done through encouraging industry's implementation of strong cryptosystems. The message between the lines was that the U.S. national security and law-enforcement interests had diverged on encryption. To be fair, part of the reason for this divergence was national security's greater ability to work around encryption, a skill that law enforcement largely lacked.

It was not altogether surprising that despite the protections built by Apple, an FBI consultant was able to unlock the device of the San Bernardino terrorist.

Other nations did not see the situation the same way. The UK government has continued to press for access to both content and devices. Australia passed a controversial telecommunications law that appears to include the government's ability to require companies to build capabilities to get around encryption—"appears" since that aspect of the law had not been contested in court at the time of this writing. Some nations, such as Russia and China, strongly restrict the use of encryption technologies. Most democratic nations do not, although discussions about doing so occur in the European Union as well as in the UK and other nations.

Returning to the issue of locked phones, it was not altogether surprising that despite the protections built by Apple, an FBI consultant was able to unlock the device of the San Bernardino terrorist. Cellebrite, an Israeli company that had started its business providing phone-to-phone data transfer, begun offering smartphone forensic tools in 2007. Police departments and governments were among its customers. In 2018, *Forbes* reported on Grayshift, a company focused on hacking iPhones whose customers included the FBI. Use of vulnerabilities to break into digital devices was not a new direction for law enforcement; the FBI had used court orders to conduct such searches since the early 2000s.

Other organizations were also successfully hacking into iPhones and Androids. The Israeli company NSO Group developed a sophisticated spyware called Pegasus that is installed through vulnerable apps or spear-phishing and, more recently, through a missed call on WhatsApp. The company claims it sells only to governments for legitimate investigations, but for over a decade NSO software has been used to target human rights activists, journalists, and political opponents of regimes (as well as their family members and friends).

In short, despite all the protections that Apple and Google had built for the phones, smartphones remained less than fully secure, especially against a determined and skilled attacker. At the same time, even when locked, the phones remained a particularly rich source of information for investigators. Users carry their mobile phones everywhere, which means that the cell tower records have approximate information of where users have been. Such proximity and location information has proved invaluable to investigators, helping them, for example, to determine the identities of a group of bank robbers simply by matching records of cell numbers with the location and time of multiple robberies.

APPS AND INFORMATION

Mobile applications also provide a lot of information. GPS tracking from map applications contains far more precise location information than cell tower sites provide. Other apps might provide other evidence. In one case, a phone showed that a suspect was using the flashlight app for an hour during the time he was believed to be burying a body in the woods. That, along with other evidence found on the same phone, provided definitive proof for his conviction.

Yet sometimes the very abundance of information that smartphones provide can thwart investigations. Smartphones store data that used to be found in other places. The scrap of paper that might have been found in a suspect's pocket listing Joe and his number is now gone, having been replaced by Joe's name and number on the smartphone's contact list—along with all the suspect's other contacts. If the user has backed up his contact list in the cloud, perhaps so he can access it on other devices, law enforcement is in luck, since the data can be collected from the cloud provider under proper legal authorization. Otherwise, information that in the past could have been so easily grabbed from the suspect's pocket may now be quite difficult for law enforcement to access, given the security protections of most recent smartphones.

This type of blockage stood in contrast to law enforcement's experience in the 2000s and early 2010s, a time when phone security protections ranged from minimal to non-existent, and police often examined phones upon arrest. Changes that occurred—increasing security and, at least in some jurisdictions, imposing requirements for a warrant prior to searching phones—created obstructions to conducting legal searches. Police were frustrated. In the U.S, FBI Director Comey's requests that Apple enable access to the phones did not get traction. Forcing Apple to open the phone of the San Bernardino terrorist would have changed the situation.

When that did not happen, the battle over encryption went briefly on hold—but it was not over. The late 2010s saw

numerous changes that brought new pressures to the issue.

WhatsApp introduced end-to-end encryption to its suite of communication applications in 2016; by that time, WhatsApp served as a platform for over 100 million voice calls daily. That transformed seamless end-to-end encryption from a niche product to a tool for the masses. The FBI continued to battle the public's use of encryption. The FBI as well as European legislators raised a new concern—child sexual abuse material (CSAM)—which has been spreading online at a rapidly increasing rate. The material was stored on cloud providers, with users sharing location information through encrypted communication apps, including WhatsApp.

During this period, cyberattacks became more dangerous. The U.S. and Israeli attack on the centrifuges of Iran's Natanz facility in the late 2000s was the first destructive attack on physical infrastructure, but it was soon followed by others, including Iran's attack on Saudi Aramco that erased the disks of three-quarters of the company's PCs. Russian cyberattacks against Ukraine were different in scale, but also showed a willingness and a capability to cause serious physical destruction and damage. Meanwhile, the incidence of ransomware exploded, often targeting critical infrastructure. While cryptography was not the only technology necessary to protect against such attacks, it was an essential piece of security solutions. Consequently, at least in the United States, which continued to be one of several nations most under attack—Ukraine was another—there was little appetite by the national security community for encryption restrictions.

During this period, cyberattacks became more dangerous. Meanwhile, the incidence of ransomware exploded, often targeting critical infrastructure. While cryptography was not the only technology necessary to protect against such attacks, it was an essential piece of security solutions.

The Carnegie Committee on Encryption

In 2018-2019, under the auspices of the Carnegie Endowment for International Peace, a group of senior former U.S. government officials worked with members of industry, civil-liberties organizations, and academia to break the impasse on encryption policy. Many of the members of the committee have assumed to senior positions within the Biden administration, including positions with direct concerns about encryption. I also note that I served on this committee.

The report of the Committee, entitled "Moving the Encryption Conversation Forward," was published in 2019 and it started by abandoning two strawmen: *one*, that society should not try for approaches enabling access to encrypted information, and *two*, that law enforcement will be unable to protect public safety unless it can access all encrypted data.

Today, encryption means many things. To make progress, those of us serving on the Committee proposed splitting the encryption problem into component parts—an approach that makes sense since encrypted communications and encrypted data are fundamentally different technical problems (access to one would not imply access to the other).

We focused on data secured on mobile phones since this issue is of greatest concern to U.S. law enforcement. Another argument for doing so is that currently no approach to encrypted communications fully satisfies cybersecurity, public safety, national security, competitiveness, privacy, and civil and human rights needs while also providing law enforcement access.

We started with principles that technical solutions for law-enforcement access must follow, noting that while we were focused on access to data on secured mobile phones, these principles also apply to other aspects of the debate (e.g., communications):

- *Law Enforcement Utility*: The proposal can meaningfully and predictably address a legitimate and demonstrated law enforcement problem.
- *Equity*: The proposal offers meaningful safeguards to ensure that it will not exacerbate existing disparities in law enforcement, including on the basis of race, ethnicity, class, religion, or gender.
- *Specificity*: The capability to access a given phone is only useful for accessing that phone (for example, there is no master secret key to use) and that there is no practical way to repurpose the capability for mass surveillance, even if some aspects of it are compromised.
- *Focus*: The capability is designed in a way that it does not appreciably decrease cybersecurity for the public at large, only for users subject to legitimate law enforcement access.
- *Authorization*: The use of this capability on a phone is only made available subject to duly authorized legal processes (for example, obtaining a warrant).
- *Limitation*: The legal standards that law enforcement must satisfy to obtain authorization to use this capability appropriately limit its scope, for example, with respect to the severity of the crime and the particularity of the search.
- *Auditability*: When a phone is accessed, the action is auditable to enable proper oversight, and is eventually

made transparent to the user (even if in a delayed fashion due to the need for law enforcement secrecy).
- *Transparency, Evaluation, and Oversight*: The use of the capability will be documented and publicly reported with sufficient rigor to facilitate accountability through ongoing evaluation and oversight by policymakers and the public.

Client-Side Scanning

These principles turn out to be quite applicable to the newest proposed technical solution to provide access to encrypted communications: client-side scanning (CSS). Such scanning has been discussed in the European Union as a possible solution to the CSAM problem.

In 2018-2019, under the auspices of the Carnegie Endowment for International Peace, a group of senior former U.S. government officials worked with members of industry, civil-liberties organizations, and academia to break the impasse on encryption policy.

Scanning of personal content is not new, but until now it has occurred on the server. As cloud storage became cheaper (indeed, often free), users could send links to where these items are stored in the cloud, instead of sending photos or documents to one another. Many cloud providers scan the content stored in their cloud. One reason for doing so is to prevent their servers from hosting illegal content or content that violates their terms of service (Facebook, for example, prohibits displays of nudity or sexual activity). Another is that they may use the information about user interests for business purposes, e.g., to serve ads.

Now, providers are moving to encrypting cloud content, making such scanning much harder. CSS would circumvent this problem, as well as end-to-end encryption, by scanning content on a user device prior to the data being encrypted or after it is received and decrypted. Currently, client-side scanning is being proposed to search for CSAM. However, the fact is that once a CSS system is installed, repurposing what it is searching for is not technically difficult. That creates a serious risk to users. Proposed CSS systems search for "targeted content" that someone has determined should not be on user devices. It could be CSAM, but it could just as easily be political material. The latter is the danger of CSS: as we know well—what one government may label as terrorist materials; another may see as free speech.

Anti-virus systems show us that client-side scanning is not a new technical innovation. But the proposed versions of CSS are substantively different from anti-virus material in a crucial way. Anti-virus software works to benefit the user, while CSS systems check if the user has content on their device that the government deems illegal—implying they do not work for the user but, rather, that they view the user as an adversary.

CSS systems rely on two types of technology to recognize targeted content on a user device. The first is machine learning, which builds models using massive amounts of data to recognize patterns. Machine learning is used in many applications, including spam filters, speech recognition, and facial recognition. The last reveals one of the problems of machine learning systems, which is a high failure rate on data substantively different from the training data. Facial-recognition systems trained on white and Asian male faces do poorly at recognizing women and Black individuals. The other technology is perceptual hashes, which produce a digital fingerprint of a media document such as a photo. If the photo is changed slightly, e.g., by rotation or cropping, its perceptual hash changes only slightly, thus making recognition possible.

Now, providers are moving to encrypting cloud content, making such scanning much harder. CSS would circumvent this problem, as well as end-to-end encryption, by scanning content on a user device prior to the data being encrypted or after it is received and decrypted.

Proponents of client-side scanning systems argue that the systems protect privacy—only targeted content is subject to legal action—while enabling law enforcement to have a workaround against encryption. But a deeper analysis shows that neither premise is correct. It is beyond the scope of this essay to discuss these technologies in detail, but I will note that both machine learning and perceptual hashes are subject to false-positive and false-negative attacks. The former occurs if an adversary produces an image that appears to match the targeted content but actually differs in substantial ways. The latter occurs if an adversary produces an image that is, in fact, targeted, but has changed the image in some minor, yet critical way that fools the algorithm (either machine learning or the perceptual hash mechanism). False positives mean that a user may appear to be hosting illegal content although he or she is not—and data on his or her devices may be subjected to searches without legal cause. At the same time, sophisticated criminals—and CSAM purveyors appear to be skilled at using modern anti-surveillance technology—will be able to evade the CSS system.

There are even more concerns surrounding CSS systems. To work, they must be installed on *all* devices, not

just those suspected of carrying targeted content. It is relatively easy to reprogram a CSS system from searching for CSAM content to searching for "tank man" photos. In other words, CSS systems can be repurposed from serving as CSAM detectors to serving as bulk surveillance tools. Think back for a moment to the principles from the Carnegie encryption policy study; it is immediately clear the client-side scanning violates several of them, including *utility*, *equity*, *specificity*, *focus*, *authorization*, and *limitation*. Many of the arguments for pursuing CSS is the inability to make targeted content public—but that same argument then presents serious problems to fulling the auditability, transparency, evaluation, and oversight principles. To put it simply, far from protecting it, CSS raises serious risks to privacy—and security.

Proponents of client-side scanning systems argue that the systems protect privacy—only targeted content is subject to legal action—while enabling law enforcement to have a workaround against encryption. But a deeper analysis shows that neither premise is correct.

Strong Encryption

The encryption debate has been ongoing for almost half a century. It started with who "owns" encryption and continued with whether the public should have the ability to keep its communications and data secure, even if that sometimes blocks legally authorized government investigations. The debate became more public and strident over the last decade, in part because the Snowden disclosures revealed far greater collection than had been understood. The wider availability of secured devices and communications, which genuinely makes investigators' jobs more difficult, contributed even more to the heated discussion.

Where do we sit at the beginning of 2022? SARS-CoV-19 turned the world upside down in 2020; one lesson we quickly learned as we transitioned to working from home was the need for widely available, easy-to-use strong encryption in consumer devices. I wrote in 2016 that, "if breakable encryption is the only permitted encryption solution, it will not only be the U.S. government that reads the communications of American companies and others, but also the Chinese, the Russian, the Iranian, the French, and many others. And they will do so with or without court orders." The proliferation of cyber exploits and cyberattacks since then serve only to emphasize the importance of availability and use of strong security through the infrastructure—and that includes strong encryption.

The New Frontier of Democratic Self-Defense

Towards A Five Eyes Cyber Collaborative

Lauren Zabierek

THE United States nor its allies alone cannot counter adversarial and criminal cyber activity in the digital domain--the reach, scale, stealth, and danger are simply too great for any one country to bear. As such, calls for international operational collaboration in cybersecurity and emerging technologies are increasing. Former U.S. State Department Cyber Diplomat Chris Painter noted in a December 2020 *Foreign Policy* article that there must be more leadership and partnership on global cyber cooperation. What follows represents a thinking-through of what this ought to entail.

Operational Collaboration

First, it's important to first understand what is meant by operational collaboration. At its core, this means conducting activities together (jointly, multilaterally, etc.) to achieve an outcome—in the context of cybersecurity, it may be defensive or offensive activities in an effort toward enhanced security and resilience. In a 2018 report entitled *An Operational Collaboration Framework for Cybersecurity*, the Aspen Institute defined this concept as the public and private sectors "working together to protect, mitigate, prevent (during steady state), and respond and recover (during an incident) with several cross-cutting enablers." As there are efforts to create opportunities for operational collaboration at a domestic level, there should be a similar focus on the international level.

There are some notable efforts aimed at state-sponsored international collaboration. Established in 2018 from the U.S. National Cyber Strategy, the U.S. State Department-led Cyber Deterrence Initiative (CDI) provides a framework for deterring and responding to malicious cyber activities nation states. At its October 2020 launch it was described by Assistant Secretary of State for the Bureau of International Security and Nonproliferation Christopher Ashley Ford thusly:

> The United States will launch an international Cyber Deterrence Initiative to build […] a coalition [of states] and develop tailored strategies to ensure adversaries understand the consequences of their own malicious cyber behavior. The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.

If the desire for stronger, institutionalized collaboration is there, why hasn't it materialized yet?

However, as Emily Goldman wrote in a recent issue of the *Foreign Service Journal*, the CDI effort has largely stalled and hasn't delivered hoped-for results, noting that its "post facto cost imposition, chiefly through sanctions and indictments, have not deterred state-sponsored actors from harming their neighbors and rivals in and through cyberspace."

More recently, the Five Eyes issued joint adversaries (the latest with guidance on mitigating the Log4j vulnerability) and have even issued a joint playbook—posted by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) as Alert AA20-245A—focused on remediating malicious activity.

Digging deeper into the Five Eye members' national cyber strategies, there are notable mentions of collaboration and interoperability with like-minded partners. The U.S. Military's Cyber Command released statements on joint training with Australia and reaffirming its bilateral relationship with the United Kingdom in 2020 and 2021, respectively. Finally, in November 2021, the U.S. joined the Paris Call for Trust and Security in Cyberspace, stating,

> Our decision to support the Paris Call reflects the Administration's pledge to renew America's engagement with the international community, including on cyber issues. We are committed to working alongside our allies and partners to uphold established global norms in cyberspace and ensure accountability for states that engage in destructive, disruptive, or destabilizing cyber activity.

Despite varying effectiveness and their ad hoc or bilateral nature, these data points are important ones, signaling the increasing desire for meaningful collaboration in cyberspace between allies.

Lauren Zabierek *is Executive Director of the Cyber Security Project at the Belfer Center for Science and International Affairs of the Harvard Kennedy School of Government. She is a former U.S. intelligence analyst and is also a co-founder of #ShareTheMicInCyber. You may follow her on Twitter @lzxdc.*

If the desire for stronger, institutionalized collaboration is there, why hasn't it materialized yet? Part of the issue may touch on the question, "what is it?" The Aspen Institute answered this question in its 2018 report, providing a useful framework for what it is, and what it should include.

The report details five distinct mission areas in steady state (protect, mitigate, prevent) and incident response (respond and recover). The same report noted four factors preventing holistic collaboration: *one*, no defined framework for organizing operational collaboration; *two*, lack of clarity regarding the relevant players; *three*, unclear roles and responsibilities of those players; and *four*, undervaluing proactive operational cooperation between the public and private sectors.

Therefore, rather than further explain what it is, in this essay I aim to provide ideas for how to address the factors listed above. Admittedly, the fourth one requires further research and observation—specifically of the EU's Joint Cyber Unit (JCU)—on an international level.

The lack of clarity inhibiting full collaboration rests on a point that I and others argued in a paper published in summer 2021 entitled *Toward a Collaborative Cyber Defense and Enhanced Threat Intelligence Structure*—namely, that, at least in the United States, the structures and the policies do not yet exist broadly. However, they are being created in the European Union through its Joint Cyber Unit.

America would do well to emulate the spirit of that framework and operate alongside the EU's Joint Cyber Unit with a structure comprising the Five Eyes nations—a Five Eyes Cyber Collaborative—given the close intelligence and law enforcement relationships the group already shares.

Here, I make the argument that America would do well to emulate the spirit of that framework and operate alongside the EU's Joint Cyber Unit with a structure comprising the Five Eyes nations—a Five Eyes Cyber Collaborative—given the close intelligence and law enforcement relationships the group already shares. Such an effort would set the table for transnational collaborative efforts, working alongside the EU's planned JCU and propagating best practices to other groups and built around the already-existing Five Eyes Law Enforcement Group (FELEG) that works together to combat cybercrime.

The notional Five Eyes Cyber Collaborative, or FECC for short, would bring each nation's cyber capabilities to bear—diplomatic, military, law enforcement, and domestic response—in a highly networked, globally dispersed, coordinated, and persistent manner.

In advocating for action on the international stage, two points come to mind. *First*, international civil society organizations are vital to recognizing issues and setting the agenda, bringing people together and exercising, and recommending policies and developing resources. Governments, however, must take a lead role to formalize and operationalize recommendations, and drive collaboration by coordinating action and bringing resources and weight to these efforts—much like the European Union has done with the Joint Cyber Unit, and NATO has done with its Cooperative Cyber Defence Centre of Excellence.

Second, while discussion of norms, policies, and laws at the strategic level is critical to defining what is acceptable behavior in cyberspace between states, we must also create structures and policies at the operational level between nations, civil society, and industry to facilitate international collaboration. While several organizations do important work in this strategic space, the operational space—particularly outside of traditional defense—is ripe for growth. As mentioned, a noteworthy example of creating those structures and policies, and housing them under a comprehensive effort is the European Union's Joint Cyber Unit (JCU), one that we would do well to replicate on a global scale.

Next, a few words ought to be said about the envisioned stakeholders involved. The Five Eyes is an intelligence partnership between the governments (traditionally between the military and intelligence communities) of the United States, Great Britain, Canada, Australia, and New Zealand. According to FBI sources, FELEG was born out of this partnership, which works together to combat transnational cybercrime. But, as mentioned, the domestic cybersecurity organizations in the member nations have also started to work together to produce joint advisories and playbooks. And given the stated desire for further collaboration, it makes sense to build the connective tissue for each nation's cybersecurity elements—military, law enforcement, domestic, intelligence, and diplomatic—to officially come together and collaborate. Doing so requires common operating policies and procedures, communications infrastructure, and platforms, and of course, people.

Building out this partnership brings all the cyber capabilities of each nation to bear in a coordinated manner; such an arrangement could complement the other's inherent strengths and weaknesses (and enhance interagency cooperation domestically) and facilitate the

institutional collaboration that members seek. In a 2020 policy paper published by the Tallinn-based NATO Cooperative Cyber Defense Centre of Excellence entitled "*The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative*," author Josh Gold states that New Zealand has stated it wants a way to better interoperate with partners in cybersecurity. In the same piece, he noted that Australia's strategy mentions the need for cooperative architecture including ways to respond within international law. Moreover, such a partnership would create a globally distributed, forward-deployed, and persistent architecture that can set norms and behavior collectively and transparently, which Emily Goldman described in her 2020 paper, published in the Fall 2020 edition of the *Texas National Security Review*, entitled "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy."

The development of norms in cyberspace is an important foreign policy endeavor.

Building on the Aspen Institute's framework and the Institute of Security and Technology's Ransomware Task Force recommendations, such an organization should have three main elements: *one*, signed agreement and active cooperation on norms between member nations (i.e., rules of the road, standards setting, capacity building, and awareness); *two*, operational collaboration (as identified in the Aspen framework above); and *three*, an engagement and communications element.

Agreement and Active Corporation on Norms

The development of norms in cyberspace is an important foreign policy endeavor. As discussions evolved from the smaller-group UN Group of Governmental Experts (GGE) process to the multistakeholder Open-Ended Working Group (OEWG) process, general, broad agreements on what constitutes responsible behavior in this domain have, at least to some extent, provided guidance for how nation-states should operate within this domain. Of course, such norms have gaps in applicability—they are non-binding, nations can find loopholes, and cybercriminals (whose increasingly sophisticated activities make them major actors in the system) will not abide by normative frameworks. Furthermore, multilateral processes have influenced the state of play to the extent that the fundamental nature of a free and open internet has been brought into question, throwing cooperation on international agreements like the Budapest Convention on Cybercrime into jeopardy.

Against this backdrop, like-minded nations must come together to agree and actively cooperate on norms and basic principles. When nations come together to agree to cooperate, it's a signal to the rest of the world.

The global cybersecurity landscape is an uneven one, with varying internal capacities and governance. As Christie Lawrence and I wrote in a September 2021 oped,

> an international body or partnership is needed to hold countries accountable while incentivizing compliance. A smaller grouping of countries could agree to a declaration that not only sets a higher bar for responsible state behavior in cyberspace, but also addresses the need for cybersecurity principles and the protection of an open, interoperable, and reliable internet.

Countries endorsing such a declaration could in turn produce national action plans for satisfying these principles. Here, the diplomatic, defense, and domestic cybersecurity elements of each nation could work together to develop these principles in tandem, beyond norms, and identify the mechanisms for agreement and accountability. As Emily Goldman writes in her aforementioned article, "norms are constructed through 'normal' practice and then become codified in international agreements. By persistently engaging and contesting cyberspace aggression, the United States can draw parameters around what is acceptable, nuisance, unacceptable, and intolerable." In this case, this burden could be shouldered by the Five Eyes members.

On the notion of acceptable behavior in cyberspace, it is imperative for like-minded states to come together and agree on activities that are and are not acceptable, and agree to abide by such a declaration. Again, using the existing Five Eyes relationship, it would be an incredibly powerful signal to declare consensus and act upon the following:

1. what is and what is not critical infrastructure (and why);
2. what is acceptable state behavior in cyberspace;
3. that cybercrime and other cyber or digital-enabled means to disrupt, degrade, or destroy critical infrastructure systems, no matter the actor, is a matter of national security and will be prioritized as such;
4. what is acceptable regarding cyber-enabled espionage.

On this last, while the aforementioned Tallinn Manual provides guidance around the applicability of international humanitarian law on cyber-enabled espionage, I propose that participating nations should come to active agreement on this activity, namely that it should meet the four criteria. *One*, the intent of spying should remain passive—to understand, to inform, and not have an active, potentially destructive or disruptive action component to it. *Two*, it should be focused on purely

government or military targets. *Three*, espionage should not be directed toward critical infrastructure and systems that people depend on to survive, as the concept of "holding [critical infrastructure] targets at risk" in cyberspace is incredibly dangerous for humanity. *Four*, in the event that malware is discovered targeting those systems, states should not deny attribution and should also offer additional information for the intent of an operation and how to stop said operation in official channels in order to prevent escalation in cyberspace, especially in the event of an operation gone wrong.

On the notion of acceptable behavior in cyberspace, it is imperative for like-minded states to come together and agree on activities that are and are not acceptable, and agree to abide by such a declaration.

To take the concept of defining acceptable behavior in cyberspace one step further, the members of what we could call the Five Eyes Cyber Collaborative could look to develop a "social contract" for cybersecurity within their nations. The "social contract" could outline what citizens and organizations can expect of their governments in terms of protections, laws, operationalization of norms, defense, and response. It would also outline what the nation needs from its citizens. Some foundational items might include—at a minimum—cybersecurity reporting requirements (that sets the foundation for information sharing and understanding the threat landscape), regulations for the cybersecurity of critical infrastructure, and data security and privacy laws. Agreements between member nations and stakeholders on regulating cryptocurrency would be another impactful step toward protecting citizens from ransomware.

Moreover, as more of the world digitizes and gets online to recover in the aftermath of the COVID-19 pandemic, there is a parallel need for cybersecurity awareness education and tools to keep people safe online and maintain resiliency that is built through achieving increased connectivity. Such efforts must work in tandem not only to further the goals for an open internet as described above, but also to protect against the malign use of information and communication technologies (ICTs) through disinformation, cyberattacks, protecting vulnerable populations against nefarious and violent activity, and the promotion of authoritarian regimes.

There should, therefore, be an agreement that members will work together to identify their educational, awareness, and outreach needs, in addition to infrastructure and capacity building needs, as outlined above. Working with existing organizations in this space, like the Organisation for Economic Co-operation and Development (OECD), would be salutary. Doing so will add a layer of standardization in order to scale efforts while still allowing for customization for each country's needs. Efforts like these—especially with outreach in the global south where the United States has long since ignored development—may help against the authoritarian wave in those regions.

The members of what we could call the Five Eyes Cyber Collaborative could look to develop a "social contract" for cybersecurity within their nations.

Operational Collaboration

Collaboration in the cyber domain is becoming a bit of a buzzword. The JCU lists its specific activities as preventing, deterring, and responding to cyberattacks through resilience, law enforcement defense, and diplomacy. As noted above, the Aspen Institute defines it as the actions taken together to Protect, Mitigate, Prevent, Respond, and Recover. But, as the Aspen Institute further notes, there are some key challenges that prevent effective collaboration. These include a lack of a defined framework for organizing entities to collaborate; the lack of clarity in both identifying the right players and their respective roles and responsibilities; and a lack of understanding how the public and private sectors can come together and conduct these activities.

In this essay, I attempt to get at some of those challenges by describing some key bucketed actions and stakeholders within a notional Five Eyes Cyber Collaborative, noting that while the Five Eyes Framework already exists, the coordination of cyber activities among member nations does not approach what the JCU is currently organizing.

The question of institutional structure is an important one. In a co-written paper for the Harvard Kennedy School Belfer Center in August 2021 that discussed collaborative defense in the United States, my co-authors and I argued for the establishment of "Collaborative Defensive Analysis Centers," housed in the ten CISA regional offices, in which cross-functional teams of analysts and network operators from the U.S. federal government as well as U.S. state governments, as well as the private and nonprofit sectors (especially those in critical infrastructure), could sit together analyzing information, provide early warning across the system, and coordinate defensive actions. As noted in the aforementioned Belfer Center paper, the CISA regional offices provide

> physical breadth for the mission and functional diversity, as well as a field office touchpoint and access for businesses and states operating within that region. Such a structure would ensure a sustained, government-led coordinated presence in all regions of the country to combat the threat on a local level. Further, this structure offers visibility, sustainability, and scale, which are vital attributes for protecting critical infrastructure from cyberattacks.

Of note, Australia has already created such a model with its Joint Cyber Security Centres, with centers in five locations across the country.

Agreements between member nations and stakeholders on regulating cryptocurrency would be another impactful step toward protecting citizens from ransomware.

In an international schema, the five member nations represent five regions, offering physical breadth (and cross-time zone operational capacity) and the ability to coordinate actions and early warning on a global scale. Much like in the military, a daily (or nightly) Operations and Intelligence Briefing would be vital to each nation's situational awareness and each of elements involved could then liaise with their reach back station.

Each nation brings to the table varying capabilities in terms of protection, response, cost imposition, exercise, and communication. Organizing those capabilities in such a way that facilitates coordination across the alliance would define the framework, and collaboration would ensure each nation complements and offsets each's strengths and weaknesses. In the EU's June 2021 JCU Factsheet, plans call for a common physical platform in Brussels to coordinate the cybersecurity actions across the EU space: the wording is "to come together to conduct joint operations, share knowledge, and work together."

Similarly, the geographic dispersal of the Five Eyes nations gives a notional arrangement physical breadth and allows for 24/7 coverage. There are already EU bodies—e.g., the European Union Agency for Cybersecurity (ENISA), Cyber Rapid Response Teams (CRRTs), European External Action Service (EEAS), and the European Cybercrime Centre (EC3)—that are focused on various aspects of the cybersecurity ecosystem. These are to be woven into the JCU, giving it somewhat of a seamless nature, which is something that the Five Eyes alliance lacks (other than FELEG). Therefore, building the connective tissue between similar bodies across the Five Eyes nations will take additional time and coordination, but would weave together the capabilities across the five eyes in resilience, response, cost, and diplomacy.

What policies and laws do we need to facilitate international collaboration? In the aforementioned Belfer Center paper, my co-authors and I discussed updating the U.S. Cybersecurity Information Sharing Act of 2015, specifically amending the minimization requirement upon private sector entities for anonymizing data and the limited liability protection clauses. We also called for a U.S. federal data privacy law and a mandatory reporting (breach notification) law. Our argument was as follows:

> These proposals aim to increase companies' investment in cybersecurity and data protection, as well as provide a framework for more honest collaboration that improves cyber defense and avoids naming and shaming companies who are exposed to cyberattacks. […] To ensure that such a law would be positive for our model, private sector entities must be reassured that data breach notifications will be met with public assistance and additional liability protections.

These proposals are focused on data security, data privacy, and data collection, which are foundational to facilitating more effective and wide-spread information sharing between the public and private sectors. In an international collaborative framework, such regulations would be especially important for data and consumer protection, liability, and situational awareness on a global scale.

Developing policy for closer international collaboration should also be prioritized. In the United States, Presidential Policy Directive 41 (PPD-41), issued in 2016, directs interagency coordination during cyber incidents—a corollary directive could be developed for concurrently working among the Five Eyes nations during steady-state and incident response activities. Similar provisions for international engagement could be described in the 2018 U.S. National Cyber Strategy and the 2016 U.S. National Cyber Incident Response Plan (NCIRP). Similar policies in each member nation would have to be developed to reflect similar guidance.

TECH

In the aforementioned Belfer Center paper, my co-authors and I stated that "collecting more threat data, and processing it to detect anomalies and create a common operating picture, is vital to the success of our cyber operations, offensive and defensive." We further noted that the "information and the technology to do this exists, but we do not have the infrastructure or the policies in place to drive coordinated, sustained sharing to create a holistic understanding of the threat at the strategic, operational, and tactical levels, as data resides siloed in countless networks."

Similarly, the EU Recommendation on Building a Joint Cyber Unit (published in June 2021) stated, that

> there is still no common EU platform where information gathered in different cybersecurity communities can be exchanged efficiently and safely and where operational capabilities can be coordinated and mobilized by relevant actors. As a result, cyber threats and incidents risk being addressed in silos with limited efficiency and increased vulnerability. Furthermore, an EU-level channel for technical and operational cooperation with the private sector, both in terms of information sharing and incident response support, is missing.

As such, this the JCU Factsheet states that it will develop "a virtual platform for collaboration and secure information sharing, leveraging the wealth of information gathered through monitoring and detection capabilities (European Cyber Shield)" which a Five Eyes framework should consider as well.

Operating alongside the JCU, the Five Eyes Cyber Collaborative would form a second operational node within a broader network of like-minded allies and partners. Where the Five Eyes already has a strong intelligence-sharing relationship, and whereas the FBI participates in the FELEG with subsequent cybercrime working groups, and whereas the FELEG has connectivity with EUROPOL and the EC3, there should be a mechanism for exchanging information as needed between the two nodes as well as coordinating defensive, diplomatic, and incident response activities across the network of the two coalitions.

As indicated in the nascent JCU's strategy document, a virtual platform is intended to be used "for collaboration and secure information sharing, leveraging the wealth of information gathered through monitoring and detection capabilities." So too should the Five Eyes Cyber Collaborative, in order to facilitate rapid communication across the group. It is unlikely that the same common technical platform would be utilized across all the nodes in the networks, but some level of connectivity between the nodes is crucial for sharing information. While the U.S. domestic cyber ecosystem is its own unique and complex system, the core of the argument rests on identifying the policies, structures, and technology needed to facilitate defensive collaboration and rapid intelligence sharing.

Such a vision is in line with the Institute for Security and Technology's Ransomware Task Force as well as the EU's proposed JCU. According to its press release,

> the Joint Cyber Unit will act as a platform to ensure an EU coordinated response to large-scale cyber incidents and crises, as well as to offer assistance in recovering from these attacks. Today, the EU and its Member States have many entities involved in different fields and sectors. While the sectors may be specific, the threats are often common—hence, the need for coordination, sharing of knowledge and even advance warning.

Using a common, encrypted platform for communications across the nodes—like between the Five Eyes Cyber Collaborative and the Joint Cyber Unit, for instance—is vital to coordinated incident response and law enforcement activities. Technology developments like differential privacy or confidential computing may enable information sharing in a way that protects privacy and security. Procedures should be established and tested during regular exercises, and of course, should be protected from cyberattacks by adversaries.

Building the connective tissue between similar bodies across the Five Eyes nations will take additional time and coordination, but would weave together the capabilities across the five eyes in resilience, response, cost, and diplomacy.

RESOURCING

It is important to acknowledge that such an organization will be incredibly resource-intensive, which would impact upon already resource-constrained nations. Members should look for ways to increase the pipeline—one suggestion is to institute a "service year" option for those people who want to get into cybersecurity but lack the means for training and certifications or need the often-requisite yet elusive year of experience at entry level.

With varying levels of resources, Five Eyes countries could further relationships in emergency management by formalizing cyber mutual aid to enable pre-incident proactive measures, as previously mentioned, and help provide subject matter expertise to enhance response and recovery activities to fully flush out attackers in governmental and private industry systems.

Further questions to consider include how to lead, staff, and fund this organization. For instance, it may make sense to build a rotating schedule (with terms at two-three years) between each of the nations. Each 'bucket' could have a director and staff to facilitate regular coordination and exercise—both internally and externally. How would this be funded and staffed? Would personnel and leadership come from career service, political appointments, detailees, or a mix? How much should be budgeted annually, and from which agency's budget would funding be carved out?

Determining the answers to these questions in each nation will take time, coordination, and political will. But the questions will need to answered.

PUBLIC-PRIVATE COLLABORATION

In the United States, collaboration between the public and private sectors is hampered by cultural, legal, structural, and tech issues. As the Belfer Center paper I co-wrote indicates:

> Sharing between the private and public sector is often point-to-point and incident-based, save for limited, voluntary coordination between Sector Risk Management Agencies and their constituents. The structures and policies are simply not in place to facilitate sharing and collaboration. […] Even when such informal connections exist, the private sector is reluctant to share information as there are no defined circumstances under which federal agencies can share information with the private sector. Fears of liability, litigation, and additional regulatory action on one end, and the lack of security and safety regulations on the other make up the centerpiece of the current legal challenges that stymie collaborative information sharing and cyber defense efforts.

Among the recommendations that we posed in the paper were to:

1. Create a Network of Collaborative Defense Centers in which cross-functional teams of analysts and operators from public and private organizations sit side by side, analyzing and sharing cyber threat intelligence, providing early warning across the ecosystem, and coordinating defensive actions with stakeholder organizations.
2. Scaling Voluntary Data Collection and Processing. This includes addressing the Cybersecurity and Information Security Act of 2015 to transfer the burden of minimization from private sector entities to a government-funded solution and granting more extensive protections to private sector entities who share information--something that was addressed in the yet-unpassed Cybersecurity Incident Reporting Act (it was left out of the final version of the 2022 National Defense Authorization Act).
3. Creating a Culture Shift to Knock Down Barriers by building trust, regular processes, and communication.
4. Unraveling the interagency challenges and addressing intelligence frameworks.
5. Addressing Personnel through Pipelines, Talent Exchanges, and Training.

Scaling up public-private collaboration globally requires addressing each of these areas, with special focus on the legal and technological components between governments and their private sectors. More research on the myriad laws within each of the Five Eyes nations addressing information sharing, data privacy, and security should be done. Moreover, given that the Five Eyes construct is an intelligence sharing partnerships, questions remain around clearances and access to information (since there are already hurdles in sharing within the organization as it is), as well as the cost-benefit analysis in doing so between nations. In the Belfer Center paper, we suggested that if clearances were not granted, then organizations must still continue to issue time-sensitive and unclassified advisories.

In the age of ambient dis-and-misinformation and instantaneous news, a collaborative effort would need an element dedicated to crafting and responding to political messaging, especially on the heels of coordinated military or law enforcement action.

DIPLOMATIC ELEMENT

The U.S. State Department stands at the core of the Cyber Deterrence Initiative. As Christopher Ashley Ford put it in his aforementioned speech from 2020, "cyber diplomacy […] seeks to build strategic bilateral and multilateral partnerships, expand U.S. capacity-building activities for foreign partners, and enhance international cooperation." The State Department is also working to build out its new Cybersecurity and Emerging Technologies Bureau, signaling its importance and the recognition that it must take a role in a Five Eyes Cyber Collaborative with more equal footing with its interagency partners; the same should go for corollary departments in each member nation.

In the age of ambient dis-and-misinformation and instantaneous news, a collaborative effort would need an element dedicated to crafting and responding to political messaging, especially on the heels of coordinated military or law enforcement action. The need for this is evident in two examples. *First*, as operations in the cyber domain offer nation states some element of plausible deniability, the ability to shape the narrative to fit the state's domestic political goals is a common action. *Second*, even cybercriminals are getting into the game of shaping global opinion; just recently, the ransomware group known as Conti (also known as Ryuk) released a statement in October 2021 denouncing multilateral law enforcement action (as a norm) and threatening retaliation.

The ability to respond to and shape messaging around activities with the support of member nations behind it will be vital to winning the public's trust and getting other nations on board with norms and rules in cyberspace.

Establishing a more extended coalition with Australia and New Zealand through this proposed arrangement

places additional diplomatic pressure to shape norms of behavior in cyberspace. Adding respective diplomatic entities to the group will enhance member nations' ability to communicate with non-democracies publicly and privately as cost imposition activity increases, as these governments will no doubt have concerns about their sovereignty and will likely respond in part by shaping the narrative of activity within their own countries along those lines. Coordinating across the Five Eyes Cyber Collaborative and member nation diplomatic corps on these efforts will ensure unity of effort and messaging in the face of a challenging international domain.

While most experts agree that attribution is not so much a technical issue as it is a political one, there is a lack of consensus concerning the threshold of evidence required for definitive attribution of cyber operations.

Additional Topics

Before coming to a general conclusion, it is useful to address a number of specific additional topics: the cyber operations attribution, the issue of prevention and resilience, incident response, and cost imposition. Each will be briefly examined in turn.

On the issue of the attribution of cyber operations, it needs to be said that while most experts agree that attribution is not so much a technical issue as it is a political one, there is a lack of consensus concerning the threshold of evidence required for definitive attribution of cyber operations. One step toward solving this problem may be to involve experts from the private sector, the think-tank community, and academia in developing attribution guidelines. Another solution may be to create a transnational standards body for attribution that would set the minimum thresholds and technical standards for attribution for public and private sector use; if parties were to agree on such thresholds and standards, the process of attribution would become transparent and indisputable (if not conclusive). This would bolster both governments' ability to attribute cyber incidents using open-source information without exposing or jeopardizing their own sources or methods.

Be that as it may, a Five Eyes Cyber Collaborative agreement on thresholds or standards for attribution (public and private sector) could have normative effects for other nations or other "nodes" within a broader like-minded coalition, by making attribution calls more transparent thereby helping to alleviate some of the political issues that inevitably arise.

The second topic revolves around the prevention/resilience dichotomy. The aforementioned Aspen Institute report describes protection as raising the collective level of security and mitigating the impact of threats through actions such as identifying critical systems and risk management, addressing vulnerabilities, developing and sharing information and intelligence on emerging threats, developing the ability to warn of attacks, implementing cybersecurity best practices, establishing contingency plans, and conducting exercises. Similarly, the JCU digital strategy describes various organizations within its Resilience bucket working to address capacity building, awareness raising and education, ensuring effective flow of information from the technical level to political decisionmakers, and security operations centers that monitor, analyze, and address cybersecurity incidents across the public and private sectors.

With a continuously evolving threat landscape, increased collaboration and trust are incredibly important in order to properly resource threat response.

Capacity-building for a Five Eyes Cyber Collaborative might also include intra-alliance technical and operational support. With a continuously evolving threat landscape, increased collaboration and trust are incredibly important in order to properly resource threat response. There are certainly different levels of expertise in various information systems that other countries within this alliance might not have. Such an alliance might help its participants evaluate each other's technical problems and in turn enable shared standards akin to the standards in play at the U.S. National Institutes for Standards and Technology (NIST) or the Center for Internet Security (CIS), U.S.-based non-profit. Operationally, the members could help each other establish more common "playbooks" to automate, alert, and detect threats as they come. Conducting vulnerability assessments, penetration tests, and combining security operations centers might be other ways of cooperation.

The third topic concerns incident response and attack mitigation—critical components of a collaborative body. While the capabilities of the Five Eyes members' computer incident response teams are relatively mature, the process around coordination between members is an area to enhance. In fact, the cybersecurity bodies of the members of the Five Eyes recently released a joint advisory on Log4j, signaling its ability and desire to work together. The JCU lists incident response as part of its core mission, describing technical

and policy enhancements to improve coordination between nations.

For referential purposes, here we can enumerate the main cybersecurity organizations in each of the member nations: the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), the United Kingdom's National Cyber Security Centre (NCSC-UK), and the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

As the nature of transnational cybercrime, reckless malware, and espionage operations rise to the threshold of threatening national security, the need for coordinated cost imposition has intensified.

The fourth and final topic is cost imposition. The need to disrupt criminal cyber operations that have significant national security consequences or are linked to broader strategic campaigns carried out by non-state groups but that emanate from outside of U.S. borders is vital. The IST's Ransomware Task Force report outlined ways that the U.S. can work with the international community on defensive actions and incident response. Furthermore, the FBI works closely with members EUROPOL's Joint Cybercrime Action Task Force and INTERPOL to conduct coordinated defensive action, such as infrastructure take-downs, arrests, rapid patching, and malware disruption, so there is already connective tissue and institutional knowledge in place between Europe and some Five Eyes members. As noted above, the FBI is part of the FELEG, which was established in 2014—working groups intended to conduct intelligence-driven joint operations on a global scale.

In other words, the stage is already set for further defensive collaboration with the annual meeting of the Five Country Ministerial (FCM) in which interior ministers from all Five Eyes countries affirmed their commitment to collaborate to fight cyber threats. As the nature of transnational cybercrime, reckless malware, and espionage operations rise to the threshold of threatening national security, the need for coordinated cost imposition has intensified. Some coordination in military, diplomatic, intelligence cyber activities between the Five Eyes is likely already happening, though it is unclear both to what extent and whether there is regular coordination with FELEG. If there is not, then greater institutionalized collaboration is required, especially where the lines between state and non-state actors, criminal versus state action, and government versus civilian targets are increasingly blurred.

Coming Together

As it stands, the tightest and most comprehensive example of international collaboration appears to be the European Union's Joint Cyber Union. Where the United Kingdom is no longer a member of the EU, creating a similar collaborative body focused on cyber among Five Eyes members, which already shares a close working relationship in military, intelligence, and law enforcement, may be a relatively easy win. Such a body, however, must go beyond intelligence sharing and law enforcement action by building structures within the alliance to focus on agreement and active cooperation on norms, capacity-building, operational collaboration across the range of cybersecurity issues, and an information element. The Five Eyes Cyber Collaborative would have touch points with the major government cybersecurity entities in the respective member nations.

While the U.S. domestic cyber ecosystem is its own unique and complex system, the core of the argument rests on identifying the policies, structures, and technology needed to facilitate defensive collaboration and rapid intelligence sharing.

Similarly, this body should operate alongside the JCU, as a corollary node in a broader coalition of like-minded nations for effective international collaboration. Other nodes could be easily added and given assistance to strengthen their cybersecurity posture in exchange for active cooperation. The broader coalition should embody a multistakeholder approach, welcoming the participation of government, private sector, and nonprofit entities. Such a framework might serve as a model for future international collaboration on issues like supply chain security.

More research and consideration must be done on private sector participation, and whether or how to include the private sector in a global, multilateral/multistakeholder approach. For instance, research on how to integrate elements of each nation's private sector—to include internet service providers, cloud infrastructure, and major software companies—and the laws or policies that might allow sharing and access to information–would be useful for decisionmakers.

EU Privacy Law and U.S. Surveillance

Solving the Problem of Transatlantic Data Transfers

Ira Rubinstein and Peter Margulies

THE July 2020 decision of the Court of Justice of the European Union (CJEU) in *Data Protection Commissioner v. Facebook Ireland, Ltd. and Maximilian Schrems* (*Schrems II*) was both a landmark in privacy law and a major obstacle for international trade. The *Schrems II* court cited the breadth of U.S. surveillance in holding that the EU-U.S. Privacy Shield agreement on transatlantic data transfers failed to provide adequate safeguards for the privacy of EU persons' data. This meant that Privacy Shield violated the EU's robust privacy law, the General Data Protection Regulation (GDPR). Both the European Commission—the EU's executive arm—and the United States are now seeking a resolution that will allow data transfers while protecting privacy.

The viability of transatlantic data transfers is a pressing and pervasive problem. Tens of thousands of companies depend on transatlantic data transfers. A halt to data flow would undermine the business models of countless firms.

Unfortunately, most current approaches to resolving the EU-U.S. conflict fall short. The Trump Administration sought to wish away the conflict, as in a September 2020 white paper by the Department of Commerce entitled "Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*." The Biden Administration has met with its European counterparts with the goal of negotiating a new agreement on cross-border data flows, but the two sides have yet to announce a successor accord. Not surprisingly, EU officials hope to avoid a "*Schrems III*" scenario in which they make concessions to the U.S. only to see the CJEU strike down a new agreement. Yet the approach of the European Data Protection Board (EDPB), which insists on rigid technological fixes that will severely hinder most transatlantic transfers of personal data, amounts to neither a practical interim solution nor a sound basis for successfully negotiating a new détente. In a forthcoming article in the *Connecticut Law Review*, we offer a hybrid approach that incorporates both substantive and institutional safeguards and a pragmatic assessment of the real-world risk of U.S. surveillance for particular data. Here, we will describe some of the suggestions we make in the paper and the dynamics that underlie the problem.

The viability of transatlantic data transfers is a pressing and pervasive problem. Tens of thousands of companies depend on transatlantic data transfers. A halt to data flow would undermine the business models of countless firms.

The Two American Measures

The CJEU's concerns started with Edward Snowden's 2013 revelations about U.S. surveillance. In the EU, worry about the scope of American surveillance centered on two U.S. measures: section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333. These enable American surveillance officials to target the communications of persons or entities reasonably believed to be located abroad to obtain "foreign intelligence information."

Section 702's definition of "foreign intelligence information" includes attacks on the United States, espionage, sabotage, international terrorism, and proliferation of weapons of mass destruction, along with a more amorphous category: information "with respect to a foreign power or foreign territory that relates to […] the conduct of the foreign affairs of the United States." Review of this surveillance is limited. In 1978, as part of the original FISA, the U.S. Congress established the Foreign Intelligence Surveillance Court (FISC), which issues court orders under FISA's "traditional" framework, authorizing surveillance of agents of foreign powers in the United States. The FISC, which comprises life-tenured Article III federal judges, approves targeting procedures under section 702 but does not approve each individual target in advance.

On its face, Executive Order 12333 requires even fewer institutional or substantive checks. The executive order itself, which dates back to the

Ira Rubinstein *is a Senior Fellow at the Information Law Institute of the New York University School of Law. You may follow him on Twitter @ira_rubinstein.* ***Peter Margulies*** *is Professor of Law at the Roger Williams University School of Law. You may follow him on Twitter @MarguliesPeter.* *An earlier version of this essay was appeared on the Lawfare blog; a longer version will appear in the Connecticut Law Review. A version of this essay was presented at an informal workshop sponsored by the staff of the U.S. Privacy and Civil Liberties Oversight Board (PCLOB). The authors wish to thank Theodore Christakis, Ron Lee, and Thomas Streinz for comments on a previous draft.*

Reagan Administration, does not expressly limit targets, except for the general requirement that these targets be located abroad. The FISC has no role in reviewing targeting protocols.

After the Snowden revelations, President Obama issued Presidential Policy Directive-28 (PPD-28), which limited the purposes of surveillance. In a nod to the growing global focus on privacy, PPD-28 acknowledged that "[a]ll persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information." Accordingly, PPD-28 limited U.S. bulk collection under Executive Order 12333 to a defined set of goals. Under bulk collection, the U.S. can collect a wide range of communications from communications providers and internet hubs—some through algorithms. Software and intelligence officials sort through these communications for those that match certain categories, including countering espionage, sabotage, terrorism, cybersecurity threats, proliferation of weapons of mass destruction, and transnational criminal threats such as money laundering and evasion of U.S. sanctions. (The guidelines released by the Office of the Director of National Intelligence in January 2021 under the title "Intelligence Activities Procedures Approved by the Attorney General Pursuant to Executive Order 12333" track these limits in more detail.)

The CJEU's concerns started with Edward Snowden's 2013 revelations about U.S. surveillance.

But PPD-28's institutional checks do not match these substantive limits. PPD-28 provided no role for the FISC, leaving Executive Order 12333 vulnerable to the same concerns that critics have levelled at section 702—that the framework lacks an independent review mechanism that would ensure that the U.S. intelligence community stays within the constraints that PPD-28 imposes.

EU Concerns

As the name suggests, *Schrems II* is the CJEU's second encounter with assessing whether U.S. law provides adequate safeguards for EU persons' data. In *Schrems I*, the CJEU in 2015 held that the then-extant data transfer agreement, Safe Harbor, failed to hedge against the scope of U.S. surveillance. After the ruling, the European Commission and the United States negotiated a new agreement—Privacy Shield—which tasked an ombudsperson at the U.S. State Department with fielding EU persons' privacy complaints. *Schrems II* found that the ombudsperson role failed to cure the problems with adequacy that the CJEU had discerned in *Schrems I*.

Schrems II cited substantive and institutional deficits in Privacy Shield that echoed its earlier ruling against Privacy Shield's predecessor, Safe Harbor. The CJEU relied on the EU's core doctrine of proportionality, which requires tailoring of government measures to actual threats. Analyzing U.S. surveillance, the court found a lack of tailoring, particularly given the apparent breadth of both Executive Order 12333 and section 702's "foreign affairs" prong. The CJEU also expressed concern that the FISC did not approve in advance all designated selectors—discrete data points, such as email addresses, social media handles, or mobile phone numbers that match individuals linked to espionage, terrorism, and so forth.

The CJEU suggested that broad discretion and technological expertise were both central to U.S. intelligence collection.

Institutionally, the CJEU stressed that EU persons' privacy complaints must be reviewed independently. The court viewed the State Department ombudsperson established under Privacy Shield as inadequate, noting that the ombudsperson was subject to dismissal by the U.S. Secretary of State. For the CJEU, independence required either a court—the preferred option—or an independent executive agency whose members were protected from dismissal.

Citing the breadth of U.S. surveillance, the *Schrems II* court also raised questions about a common workaround implemented after *Schrems I*: the so-called standard contractual clauses (SCCs). Through SCCs, companies that transfer personal data can agree to additional safeguards against government surveillance. In theory, "appropriate" safeguards can compensate for substantive and institutional deficits in a surveillance regime. The CJEU did not rule out reliance on SCCs but warned that they were not effective against a surveillance regime that featured both broad legal authority and technical sophistication. The efforts of private parties through SCCs might be futile against such a formidable regime. Underscoring its wariness, the CJEU suggested that broad discretion and technological expertise were both central to U.S. intelligence collection.

EU Countermeasures

An October 2020 decision by the CJEU, *La Quadrature du Net and Others*, expressed a more comprehensive understanding of the national security imperatives driving U.S. surveillance. In *Quadrature du Net*, the CJEU recognized that some bulk collection of information on the duration and location of communications might be necessary to ferret out evidence of existential threats such as terrorism. However, *Quadrature du Net* observed that the

core EU values of proportionality and independent review still controlled how governments picked specific real-time surveillance targets. Along these lines, two professors in European law, Theodore Christakis and Kenneth Propp, in a March 2021 *Lawfare* article describe France's efforts to revise the EU ePrivacy Directive to bypass the CJEU's regulation of national security surveillance by EU member states.

In addition, *Schrems II* opened the door for companies transferring data in-house or with contractual partners to derogate—that is, grant a limited exception—under Article 49 of the GDPR. Under Article 49(1)(b), a transfer to a country without adequate protections for data can still take place, even without "appropriate safeguards" such as effective SCCs. But a transfer must meet one of several conditions. For example, a transfer of personal data could be "necessary for the performance of a contract between the data subject" and the transferor—which could be true of, say, a U.S. company with an EU office that is transferring data about an employee. Judge Thomas von Danwitz of the CJEU has suggested that Article 49 derogations were worthy of exploration for companies that required a measure of flexibility. But the Article 49 contractual exception would not fit other contexts, such as Facebook's myriad uses of its users' personal data for targeted advertising. In other words, Article 49 offers help to firms trying to navigate EU privacy law after *Schrems II*, but Article 49's narrow scope will limit its application.

In sum, the EDPB's recommendations are either unrealistic, even for state-of-the-art data security, or undermine the very rationale of secure data transfers.

The narrow relief provided by Article 49 derogations becomes even more problematic in the context of the broad reading of *Schrems II* adopted by an important EU privacy body, the European Data Protection Board. The EDPB's Recommendations on Supplementary Measures, adopted in November 2020 and revised in June 2021, take a de facto absolutist stance that would effectively bar many of the most useful types of transatlantic data transfers, sending EU-U.S. trade into a tailspin. For example, the EDPB requires technical measures such as sweeping encryption. Under the EDPB's guidelines, a data exporter may have to encrypt data in such a way that a data importer is unable to decipher it, rendering the data transfer all but pointless. Furthermore, an EU firm may store encrypted data with a U.S. cloud service provider, but only if the encryption mechanism precludes the service provider's access to transferred data including for value-added services offered by European cloud services.

This guideline pits privacy against data security. The Board's steep encryption requirements bar cloud services from checking data transfers for malware or other cyber intrusions, which has the effect of imperiling the security of all data users. This counterintuitive result exalts privacy rights as a matter of formal law but in practice sacrifices the actual privacy of users. In a world of persistent cyber threats, the EDPB's guidance on this score seems particularly shortsighted.

The EDPB's absolutist approach stems from an unduly broad reading of Schrems II. But narrow readings of the decision also provide flawed guidance.

A case study in the EDPB's recommendations exemplifies its rigid approach. In sending EU persons' data to a "third country"—one outside the EU, such as the United States—the company must ensure that the encryption algorithm is "implemented correctly and by properly maintained software without known vulnerabilities" and is "robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities." On the surface, this recommendation seems entirely appropriate. Digging deeper, though, questions arise. The recommendation subjects data security to unrealistically high standards. While encryption is often effective, even the best encryption can suffer some flaws in implementation. Moreover, data exporters are in no position to assess the resourcefulness or technical prowess of cryptanalytic services. The Snowden revelations made this clear.

Second, the EDPB's recommendation defeats the purpose of a great deal of data transfers. Imagine that a U.S. firm with EU employees transfers data to its U.S. parent company, which needs the data to implement its human resources policies. If the data were flawlessly encrypted and transmitted to the U.S. in a packet impervious to inspection, no one at the parent company would be able to read the data—rendering the transfer pointless. In sum, the EDPB's recommendations are either unrealistic, even for state-of-the-art data security, or undermine the very rationale of secure data transfers.

The EDPB's absolutist approach stems from an unduly broad reading of *Schrems II*. But narrow readings of the decision—including those offered by the U.S. government and distinguished American commentators—also provide flawed guidance. During the Trump Administration, the Commerce Department—following the Obama Administration's approach—stressed the checks in U.S. surveillance law. In the aforementioned September 2020 white paper, the Department argued that "[m]ost U.S.

companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the CJEU in *Schrems II*." Writing in *Lawfare* in December 2020, Washington, DC-based privacy and cybersecurity attorney Alan Charles Raul argued that section 702 barred the United States from intercepting messages from the email systems of U.S. firms, even if those emails were sent or received by foreign nationals outside the United States.

Unfortunately, these narrow readings fail to pass muster. While U.S. surveillance law includes checks and balances, the CJEU focused on the absence of systematic FISC review of individual section 702 selectors—and that absence will continue to be telling, despite the presence of other limits on U.S. surveillance. Similarly, as a practical matter the risk may be low that the United States will seek to intercept emails from foreign national employees of U.S. firms. However, that is a back-of-the-envelope risk assessment, not a definitive statement of law. The CJEU signaled in *Schrems II* that exclusive reliance on risk assessment is not sufficient in the absence of concrete changes in the U.S. legal framework.

Looking to intelligence community privacy officers to review EU persons' privacy complaints is also not an adequate response to the CJEU. Privacy officers in agencies such as the National Security Agency do extraordinary work, building and maintaining a rule-of-law culture within the intelligence community. However, since U.S. privacy officers work in executive branch agencies directly answerable to the U.S. President, those officials lack the independence that the *Schrems II* court regarded as essential. Privacy officers can play a role, but their efforts are not a complete response to the CJEU's concerns.

Our Hybrid Model

Given the problems with both the broad and narrow readings of *Schrems II*, we propose an alternative: a hybrid strategy that pairs more detailed and methodical risk assessment with new institutional and substantive checks on U.S. surveillance.

To craft a more nuanced risk assessment, we look to U.S. export control law. U.S. law imposes a graduated system of controls on U.S. exports of technology and other goods, depending on conditions in the receiving state. This graduated approach may also allow for more efficient safeguards on data transfer.

EU and U.S. controls on "dual-use items"—goods, technology, or software with both civilian and military applications—are similar in most relevant respects due to European and U.S. participation in multilateral exports regimes. Export controls serve national security and foreign policy goals and deter proliferation of weapons of mass destruction. Specifically, national security controls limit foreign access to the most sensitive U.S. weapons and technology. These controls reflect the Cold War assumptions of the Coordinating Committee, a multilateral organization formed at the end of World War II by the U.S. and other NATO members to stem the flow of Western technology to the Soviet Union, its Warsaw Pact allies, and China.

Given the problems with the broad and narrow readings of Schrems II, we propose a hybrid strategy that pairs more detailed and methodical risk assessment with new institutional and substantive checks on U.S. surveillance.

Several U.S. agencies participate in export controls. Most U.S. exports are shipped abroad under general export licenses from the Department of Commerce, which require no application or prior approval for their use. The Commerce Department can also issue an individual validated license to a particular firm, authorizing exports of specific items to a particular country of destination and for specific end users and end uses.

The State Department regulates the export of items specifically designed for military purposes—categorized as munitions—under a far more restrictive regime, requiring firms to register as arms exporters and obtain individual licenses for all destinations. Many more countries are restricted as compared with Commerce Department licensing, and there are fewer exemptions. Finally, the Department of Treasury administers foreign asset controls or embargoes, which prohibit virtually all financial and trade transactions with embargoed countries such as Iran and North Korea. These are subject to limited exceptions for humanitarian aid and informational materials.

The Commerce Department's graduated approach provides the closest analogy to a comparative assessment of data protection. The Department's Bureau of Industry and Security (BIS) organizes countries into four country groups (A, B, D, and E) based on particular reasons for control. For example, Country Group A is the least restrictive group and includes key U.S. allies and members of NATO, among others; Country Group B is a catch-all for more restrictive controls; Country Group D covers about 40 countries (including China, Russia, and Yemen) that raise national security, nuclear, chemical-biological, or missile technology concerns; while Country Group E is the most restrictive and

includes countries subject to comprehensive embargoes (Cuba, Iran, North Korea, and Syria).

Like the GDPR, which serves the dual objectives of safeguarding fundamental rights to data protection and the free flow of personal data within the EU, export controls seek to limit access to strategic goods and technologies by potentially hostile countries without unduly burdening international trade. BIS controls establish general licenses for exports to many countries without the need for a license application or government approval—another echo of the GDPR, which permits data exports with appropriate safeguards to countries that have not received an adequacy determination. Finally, just as the EDPB recommendations require a firm to determine whether safeguards are "effective in light of all circumstances of the transfer," firms under the export control regime determine for themselves whether a proposed export of a dual-use item is eligible for a general license to some or all destinations or requires an individual validated license. Exporters must understand the specific conditions and restrictions of the various general licenses, how they apply to the proposed export, and when the use of such licenses is prohibited.

Dual-use export controls have practical advantages. They permit firms to classify themselves based on their own experience and expertise, which curbs heavy-handed government regulation and promotes efficiency. But the regime reserves for the government vital policy questions such as the identification of particularly sensitive export items and high-risk countries.

To adapt this process to assessments of the adequacy of data protection, EU officials—ideally accompanied by member state representatives—should conduct bilateral meetings with officials of importing countries, including the United States. Officials at the meetings would conduct comprehensive reviews of foreign surveillance laws and practices. They would also assess judicial oversight and international commitments.

The meetings would take on several specific tasks to achieve these goals. Officials should identify which of an importing country's surveillance laws permit government access to transferred data and determine what, if any, categorical legal protections exempt specific end users and end-use scenarios from the reach of these laws. They should share information about the actual practices of intelligence agencies, together with company disclosures of various statistics related to government requests for user data, records, or content. And, finally, they should consider implementing a wider array of supplementary measures along with notification procedures.

For example, imagine an agreement on guidelines under which any data exporter that relies on a risk-based assessment of third-country access as the basis for data transfers would—except in cases barred by law—receive a notice when a data importer or service provider becomes subject to a foreign government access request. This would allow the entity to revoke encryption keys and immediately suspend transfers pending the outcome of the request. The firm could also reassess the risks of relying on SCCs to accomplish such transfers. The June 2021 European Commission Implementing Decision on SCCs for the Transfer of Personal Data to Third Countries adopts this approach by requiring data importers to notify data exporters of legally binding requests for government access.

Applying the export control model to data transfers would make risk assessment far more granular, comprehensive, and reliable.

Applying the export control model to data transfers would make risk assessment far more granular, comprehensive, and reliable. Instead of the amorphous risk assessments offered by government agencies and commentators in the wake of *Schrems II*, EU data regulators could rely on a more systematic and dynamic approach, capable of shifting quickly based on changing circumstances. This approach would be a useful alternative to the EDPB's unmanageable absolutism.

Pairing with this more methodical approach to risk assessment, our hybrid model proposes institutional and substantive reforms in U.S. surveillance law. In the institutional realm, the U.S. Congress should establish an Algorithmic Rights Court that will field EU persons' privacy complaints. The court would be staffed by life-tenured federal judges and aided by a full-time public advocate who would push back on government positions. It would provide gold-standard independent review, as the CJEU requires. As a fallback position, if establishing the court is too heavy a political lift, the United States could delegate review of EU persons' privacy complaints to either the FISC—as professors Kenneth Propp and Peter Swire propose in an August 2020 *Lawfare* article—or an independent multimember executive branch agency such as the Federal Trade Commission or the Privacy and Civil Liberties Oversight Board, whose members have "for-cause" protections against dismissal.

As a substantive check, the U.S. Congress should enact a statutory presumption against collection of the communications of foreign employees of U.S. firms located abroad. Since a great deal of transatlantic data transfer concerns such employees, a statutory

presumption would install legal protections against unchecked surveillance of such persons. The U.S. government can overcome the presumption with specific evidence of a foreign employee's conduct. Furthermore, the U.S. Congress should also revise the "foreign affairs" prong of FISA section 702 to limit surveillance to actions of foreign officials. The reduced scope of the "foreign affairs" prong will reassure EU bodies that the United States is taking global privacy protections seriously.

A hybrid approach would also make derogations under Article 49 of the GDPR more practicable. Derogations to fulfill contractual duties would be more sustainable, given a granular risk assessment and added U.S. safeguards. Some commentators read Article 49 as authorizing only occasional data transfers. The assurance added by a heightened risk assessment and further U.S. safeguards could justify more regular use of Article 49. This shift would increase the flexibility of data protection regulation without sacrificing privacy.

The hybrid model may not satisfy all stakeholders, and both broad and narrow readings of *Schrems II* will continue to attract acolytes. But the hybrid model acknowledges the core insights in *Schrems II* while enabling essential economic activity. That is a scenario worth pursuing on both sides of the Atlantic.

EUROPE'S QUEST FOR TECHNOLOGICAL POWER

HIGH-PERFORMANCE COMPUTING AND QUANTUM COMPUTING

Alice Pannier

COMPUTING power plays a key role in enabling data analytics and machine learning, in cybersecurity, for scientific research, and in military domains like nuclear warhead design and detonation simulation. Computing also has industrial ramifications, not least due to a relatively small number of players that hold key spots in the value chain. This leads some to argue that the contours of computational power define who has control over and access to the benefits of computer-based technologies like artificial intelligence.

This essay focuses on two complementary segments of computing: high-performance computing (HPC, also known as "supercomputing"), and quantum computing. Both are very distinct in terms of maturity. HPC has been widely used in scientific research, meteorology, the military, finance, and industry since the 1990s. Arguably, a nation's ability to deploy supercomputers constitutes a form of soft power, as well as being a scientific and national security imperative. Today, a few countries around the globe are engaged in a race to deploy the next level of supercomputers, known as exascale machines. But the field is also currently witnessing a diversification of uses, with new needs stemming from big data applications for industry.

Meanwhile, quantum computing is still at an experimental stage but has highly disruptive potential, in both civilian and military domains. It seeks to exploit the properties of quantum mechanics and as such, constitutes a whole new paradigm in computing. Indeed, quantum computing indeed will multiply computing power exponentially, with considerable cybersecurity implications and industrial and scientific applications. The field has experienced swift progress in recent years, even if large-scale quantum computers might still be a decade away.

Alice Pannier *heads the Geopolitics of Technology program at the French Institute of International Relations (IFRI). She previously held the position of Assistant Professor in International Relations and European Studies at the Paul H. Nitze School of Advanced International Studies (SAIS) at Johns Hopkins University. This essay is based on a longer study entitled "Strategic Calculation" published by IFRI in October 2021. You may follow her on Twitter @AlicePannier.*

The race for computing power, including quantum computing, has become a key element of the U.S.-China technological competition. Yet, the competition is far from being solely a U.S.-China matter. For logical reasons considering its applications and implications, computing power is a strategic priority for European governments as well as for the European Union. This is especially the case when it comes to quantum computing. Countries around the world have recognized that quantum science has moved from an academic field of research to a fast-growing technological sector. Consequently, they are developing strategies in the field, so that current dynamics are akin to a space race.

Computing power plays a key role in enabling data analytics and machine learning, in cybersecurity, for scientific research, and in military domains like nuclear warhead design and detonation simulation

This essay examines the state of play of technological developments and international competition in HPC and quantum computing, with a particular emphasis on where France and Europe stand in the global race for computing power. The first half of the essay presents current dynamics in the HPC sector: on the one hand, the enduring role of states in shaping supercomputers as a strategic sector, and on the other hand, the ongoing "democratization" of the field, with growing uses in industry. It then then addresses the geopolitical considerations that supercomputing raises for Europe, as well as ongoing strategies aimed at enhancing Europe's technological power in the field.

The second half of the essay addresses quantum computing. After introducing the main principles of quantum computing, it reviews recent progress and remaining technological hurdles, as well as the strategic and economic applications and implications of quantum computing. It then looks at the quantum strategies deployed by the U.S., China, and EU countries, with a particular emphasis on the French 2021 Quantum Plan.

This essay shows that HPC and quantum computing present both opportunities and challenges for European countries as they seek to leverage the potentials of computing power for

the data economy and national security, as well as for addressing critical societal challenges in areas of health and climate change. Aside from national strategies and investments in HPC and quantum technologies, collective efforts in Europe to pool resources are ongoing. The EU is indeed striving to develop federated computing services and data infrastructure, and to secure resilient supply chains in components, technologies, and knowledge, not least to limit risks of disruption.

Computing technologies raise challenges for Europe—from the supply of chips to energy consumption—as well as risks, from export restrictions to company takeovers. Yet in both HPC and quantum computing, procurement choices challenge Europe in its internal debates and contradictions when it comes to developing its technological power, as the line between scientific research and strategic advantage gets blurred. Europe is also facing a well-known problem of lack of private investment in disruptive technologies. Quantum technologies do offer an opportunity to learn lessons from past developments in the field of classical computing, and to take the right actions early on. If Europe fails, it will have not only economic but also serious security implications.

In both HPC and quantum computing, procurement choices challenge Europe in its internal debates and contradictions when it comes to developing its technological power, as the line between scientific research and strategic advantage gets blurred. Europe is also facing a well-known problem of lack of private investment in disruptive technologies.

Trend in High-Performance Computing

High-performance computing (HPC) refers to computer systems often called "supercomputers" with extremely high computational power, able to solve very complex problems at high speed. The development of supercomputers has been and remains largely state-driven, as their acquisition and running costs are high and as they have uses in national security (e.g., nuclear simulation), scientific and medical research, and climate modelling. Nonetheless, the rise of the big data economy and the computing power required to train Artificial Intelligence (AI) algorithms and to run simulations, together with the growth of cloud computing, have "democratized" the recourse to high-performance computing in industry.

Today, U.S. computer and processor companies dominate the market in Europe, while China has developed indigenous technology. Europe is seeking to catch up by supporting its industrial base and developing its processor technology but is facing internal hurdles that are industrial, technological, and political.

The current concept behind high-performance computers appeared in the late 1980s-early 1990s with the advent of massively parallel processing, whereby supercomputers started to be built with hundreds of thousands of processing cores. The chart below shows the pace at which computing power has grown from the 1990s onward as a result. Computing power in the HPC jargon is measured in floating point operations per second (flop/s). While it was previously measured in gigaflop/s (i.e., one billion (10^9) operations per second), computer power is now measured in petaflop/s (10^{15} operations per second) and the standard is about to shift to exaflop/s: 10^{18} or one quintillion (one billion billion) operations per second. To provide an indication of scale, a petaflopic supercomputer is about one million times more powerful than a high-end laptop.

High-performance computing (HPC) refers to computer systems often called "supercomputers" with extremely high computational power, able to solve very complex problems at high speed.

Performance Development

Governments have historically played an important role in the development and growth of computer technology, especially HPC technology—even if, in recent decades, computer chip development has been mainly driven by the private sector, not least by the smartphone industry. The public sector is still the main consumer of concentrated computing power today.

In 2018, in Europe, over 90 percent of HPC operating time was by universities or academic research centers, whereas the remaining 10 percent served commercial purposes and end users. Chief among state-driven uses of computing power are national security uses: supercomputers can be used to design, develop, manufacture, and test weapons (including nuclear weapons) and weapons platforms; collect, process, analyze, and disseminate intelligence; for cryptography; for combat simulation; for missile defense, etc. Supercomputers are also used for weather forecasting and scientific research, including medical research. The COVID-19 pandemic is said to have engendered new needs, for biomedical applications, new drugs development, and digital twins of humans.

Since supercomputers have dual applications, they have been subject to export restrictions since the 1990s. Today, the U.S.-Chinese competition clearly plays out in the realm of HPC, due to

concerns about both intellectual property and the potential uses that can be made of U.S. chip technology. In April 2021, the Biden administration added several entities involved in HPC to the Entity List, including China's National Supercomputing Center (which is involved in the simulation of hypersonic vehicles). This prevents export of U.S. technology to such entities.

Global Distribution of Computing Power

Across the globe, a small number of countries possess significant supercomputing capabilities. China and the U.S. lead the race, followed by second tier HPC powers: Japan, Germany, France, Netherlands, Ireland, the UK, and Canada. In terms of companies, in the HPC sector, the top three vendors are Lenovo (China, #1 vendor worldwide, with 36.8 percent market share), Inspur (China, 11.6 percent), Hewlett Packard Enterprise (HPE, U.S., 9 percent), Sugon (China, 7.8 percent) and Atos (France, 7.2 percent). If we include Cray, which HPE acquired in 2019, and which holds 6.4 percent of the market, HPE has moved up to the second place, with 17.4 percent. The picture changes if one looks at computer performance rather than market share. Then, the first player is Fujitsu (Japan, 19.8 percent). The *Fugaku*, unveiled in June 2021, is the most powerful machine in the world. It has three times the power of the second most powerful. Its computing power is equivalent to 20 million smartphones combined, and it is halfway towards the exascale.

Public sector institutions—whether government departments or university research laboratories—possess the most powerful machines. Nvidia and Eni (the Italian oil and gas company) appear as two notable exceptions in the top-ten list. Aside of the top ten, we find large digital companies, and in particular cloud service providers, like Microsoft Azure's and Amazon Web Services, which have acquired significant computing resources of their own. Weather forecast agencies also rank high as HPC users across the globe.

The performance of a supercomputer for a given task depends not only on the number of the machine's cores and on the speed of the interconnecting network, but also on the type and architecture of its chips. One difficulty with HPC is that higher performance tends to come at the cost of flexibility: hardware built for specific purposes outpaces general purpose computers. Thus, many countries (the U.S., Canada, Japan, the UK, Germany, or France) have recently acquired large calculation instruments specifically dedicated to AI for their research communities. This includes the RIKEN Center in Japan, which developed the *Fugaku*; the Joint Academic Data Science Endeavour (JADE) in the UK in 2018; or the GENCI (*Grand équipement national de calcul intensif*) in France, which inaugurated a new machine for AI research (the *Jean Zay*), in 2020.

It is thus essential to consider the processors that enable HPC machines and the central role that chip manufacturers (AMD, Intel, or Nvidia) play in shaping and structuring the realm of computing power. The international landscape of processors has greatly evolved over the past few years, with the breakthrough of Nvidia, a Californian company created in 1997. Computers rely on central processing units (CPUs), as well as increasingly on graphics processing units (GPUs), which allow visual computing (such as 3D, video, computer vision and image recognition). Nvidia designs GPUs, originally aimed at the gaming industry, and which now equip supercomputers around the world. Indeed, GPUs turned out to accelerate significantly computing power for certain applications like machine learning. As such, they constituted a real revolution in HPC. In 2017, Nvidia launched a GPU based on a new architecture ("Volta"), designed for AI and especially for self-driving cars, which now equips America's two most powerful supercomputers, *Sierra* and *Summit*. The company also started manufacturing its own supercomputers. Nvidia hoped to acquire ARM, a British, world-leading chip designer acquired by Japanese holding SoftBank in 2016 for £24.3 billion (€29 billion). But as of late January 2022, press reports indicate that Nvidia is preparing to abandon its acquisition, given the lack of progress made in convincing the UK government not to block the sale due to anti-competitiveness and national security concerns, in a context of heightened geopolitical competition surrounding computer chips.

The world of high-performance computing is characterized by a race for the development of exascale computers. Exascale machines will be twice as powerful as the world's most powerful machine to date, and twenty times more powerful than the best European machine.

Toward an Exascale Machine

Currently, the world of high-performance computing is characterized by a race for the development of exascale computers. Exascale computers will be capable of carrying out one billion (one quintillion) operations per second. In other words, exascale machines will be twice as powerful as the world's most powerful machine to date, and twenty times more powerful than the best European machine. Exascale machines will make a difference in specific areas of simulation and 3D visualization used in

nuclear power research (e.g., next-generation nuclear warheads), climate sciences (e.g., forecasts of the consequences of temperature changes), high-resolution meteorology and oceanography, as well as biological and medical research (e.g., cardiac physiology). But a country's place in the world's computing power rankings are also an expression of national sovereignty and a soft power tool, as suggested by Emmanuel Jeannot of INRIA.

There are no exascale machines deployed today, but government programs are underway in the United States, Europe, China, and Japan. Developing exascale machines is a matter of cost as well as a matter of access to technology. The latter is a particular problem for China due to export restrictions of U.S. technology. As for the cost, it is illustrative that the R&D funding for the *Fugaku* has been around €1 billion over 10 years.

Very recently, China and the United States have made their own exascale machines operational. In July 2015, former U.S. president Barack Obama launched a National Strategic Computing Initiative calling for the accelerated development of an exascale computing system that integrates hardware and software across a range of applications representing government needs. HPE Cray delivered its first exascale computer, *Frontier*, to the Oak Ridge National Laboratory (ORNL, attached to the Department of Energy) in late 2021. ORNL already hosts *Summit*, which ranked as the world's most powerful machine in 2018-2020.

Given its costs and possible uses, HPC was not a critical business need for many companies until the emergence of the big data economy. Today, the functions of computing power are changing, and HPC is 'democratizing,' as it plays an important role in facilitating the development of the big data economy.

While China did not have a single supercomputer in 2001, it superseded the U.S. in terms of performance and number of supercomputers worldwide in 2016. Today, China now owns the highest number of the Top500 supercomputers worldwide, even if its machines are less performant than American ones, overall. China's first exascale machine, based on indigenous technology, became operational in late 2021, which made it the first nation to operationalize an exascale computer. In addition, Beijing has included a target of having 10 national exascale supercomputing centers in its 14th Five-year-development-plan spanning 2021-2025.

Other countries around the globe are seeking to build exascale machines, but they are less advanced than China, the U.S., or Japan. This list includes South Korea, which is aiming for a national exascale computer, relying on Korean processors, by 2030. Europe, for its part, is seeking to deploy exascale machines by 2022-2023, as we shall see below.

'Democratization' of HPC

Given its costs and possible uses, HPC was not a critical business need for many companies until the emergence of the big data economy. Today, the functions of computing power are changing, and HPC is 'democratizing,' as it plays an important role in facilitating the development of the big data economy. Indeed, with the proliferation of data, there is growing demand for extracting insights from such big data, and for near-real time analysis. HPC is especially attractive for AI technologies such as deep learning. They require a lot of computing power, so much so that the amount needed worldwide to train AI programs doubles every 3.4 month.

HPC-enabled big data analytics and simulation have plenty of uses in industry and in all design and manufacturing processes: digital twinning, design customization, operations management, maintenance, optimization, or assessment. HPC-based simulation is also relevant for 3D simulation of fluid dynamics, in driving simulation for autonomous vehicles, for tank simulation in the oil and gas business, in finance for the optimization of portfolio risk management, in crisis management scenarios (e.g., forest fires), etc.

Besides industry, growth in uses of HPC and digital twinning continues to be driven by research, including medical research and climate sciences. In fact, the need for computing power in science is ever growing. By way of illustration, since 2020, Japan has been using its *Fugaku*, to simulate the spread of COVID-19. In the future, digital twinning of the human body, based on individuals' DNA, will in theory allow medical treatments to be tailored to a person's physiology and needs.

When it comes to climate, the EU launched its "Destination Earth" (DestinE) project in 2021, as part of its Green Deal plan. The plan is to create digital twins of the Earth to simulate the effects of climate change, through a high precision digital model of the Earth to monitor and simulate natural and human activity. The project will span 2021-2030. By 2025, the project will include a cloud-based platform, with four to five operational digital twins.

Due to the generalization of its uses, the market for HPC has become quite dynamic: its growth rate for businesses has been estimated at +9.8 percent from 2017 to 2022. Market turnover reached

$41 billion (€35 billion) in 2020 worldwide and is expected to reach $66.5 billion (€56.7 billion) in 2028.

Aside from greater demand, the growth of the HPC sector is fueled by sinking costs and the greater affordability of hardware, as well as the move of HPC from "on premises" to (partly) on the cloud, whereby HPC users can access high-speed data processing from commercial services such as Amazon Web Services. A report suggests that the on premises HPC market, worth $24 billion (€20.5 billion) in 2020 and will grow at 7 percent a year by 2024, while the HPC cloud market was worth only $4.3 billion (€3.7 billion) in 2020 but will grow at 17 percent a year until 2024. As an indication of these trends, the world-leading, Taiwan-based chip manufacturer TSMC expects that, due to "unprecedented demand for compute power in cloud datacenters and communication infrastructures, […] the main driver of its growth in the next several years [will] be high-performance computing, overtaking its current smartphone business."

Is Europe Catching Up?

In 2018, the President of the European Investment Bank (EIB) regretted that "while a third of the global demand for HPC capabilities comes from European industry, SMEs, and researchers, […] only 5 percent of […] HPC capabilities [were] being provided by European HPC centers." Europe hosts one main player in supercomputing—Atos—but it is seeking to host more machines on the continent through collaborative ventures, and to develop capacities in areas of the HPC value chain where Europe is largely absent, notably processors.

The French company Atos-Bull is the sole European supercomputer hardware company. It is the result of successive French governments' objective to be sufficiently industrially autonomous to develop and maintain nuclear weapon systems. This goal drove France's post-World War II techno-industrial planning in telecommunications, atomic energy, space capabilities, and computer science. Another motivation to have a French supercomputer company was the U.S. embargo on the export to France of state-of-the-art computer equipment, for fear that the equipment could possibly fall into Soviet hands. When Bull was taken over by General Electric in 1964 and left Western Europe with no challenger to U.S. companies in a strategic sector, France launched its "*Plan Calcul*" ("computing plan") to support the emergence of a French national champion in computing. The Plan failed to create a new industrial actor from scratch, but Bull was eventually nationalized in 1982 and re-privatized in 1994. Finally, Atos took over Bull in 2014.

For the past two decades, Bull (now Atos-Bull) has been an important player in the supercomputer business. Since 2001, five years after it launched its nuclear simulation program ("*Simulation*"), the French Alternative Energies and Atomic Energy Commission (CEA), which oversees the French nuclear deterrent, has endeavored to have a "sovereign" national industry of supercomputers. The CEA got into a partnership with Bull, which delivered its first machine to the CEA (the *TERA-10*) in 2005. By 2012, Bull had three machines in the world's top 20. Today, Atos-Bull continues to provide the CEA with *Simulation*, and the French Ministry of Armed Forces more broadly for other uses. Nowadays, the need for 3D computing for future generations of nuclear weapons is what is driving the search for ever more powerful computers and the pursuit of exascale machines.

Today, both the United States and China are keeping their respective markets closed to foreign vendors.

But Atos and other European companies are not present all along the production cycle for supercomputers. Atos has its own interconnection system (BXI) but relies on non-European manufacturers for processors: the U.S.-based companies AMD, Intel and Nvidia. As suggested by a representative of Atos, the company is indeed "agnostic" when it comes to Processing Unit providers. French and EU authorities have, however, identified the absence of a European provider as a problem and sought to develop alternatives. In 2019, the head of the CEA's military arm estimated that, while the CEA has been working with Intel, in the future, there should be "a sovereign European processor," because France would "not want to be subject to an inability to have these processors."

Another problem is public procurement choices. Government procurement programs are a key determinant of HPC hardware providers' outlooks. This is especially true when companies have little chance to sell into foreign markets. Today, both the United States and China are keeping their respective markets closed to foreign vendors. In the U.S., the domestic industry is currently strongly supported with a "Buy-American" requirement for the purchase of supercomputers. A European company like Atos thus cannot hope to export its machines to the U.S. or China, and its market is largely located in Europe (UK included), Brazil, and India. What is more, unlike in the U.S. or China, public procurement in the EU is open to non-EU entities, a practice that does not always favor local providers. It is indeed striking that the *Jean Zay*, the CNRS's largest and most recent supercomputer, is HPE-built, and not Atos-built. New initiatives aim

at boosting the European HPC sector (see below), but debates have arisen about whether to give precedence to EU-based options in public procurement choices. This may change with the International Procurement Instrument, a new piece of legislation currently being negotiated in Brussels, and which would introduce a principle of reciprocity in the openness of public procurement markets, in response to legislation such as the "Buy American" Act.

A further limitation is the absence of European companies in cloud-based HPC services. Cloud-service suppliers in Europe remain largely American companies. For example, the French firm Atos has partnered with Google Cloud to provide a hybrid cloud solution for data analysis and machine learning. This is not without problems for data security. Consequently, the EIB has pushed for the development of European cloud offers, including HPC applications.

Europe, finally, has a funding problem. The European Investment Bank in 2018 called for significant investments to be made in infrastructure, access to big data, and tailor-made complex software solutions. Mariya Gabriel, then Commissioner for Digital Economy and Society, identified a funding gap in European HPC of €500 million to €750 million per year, compared to the USA, China, or Japan. One conclusion of the report was that no single country in Europe by itself has the capacity to sustainably set up and maintain an exascale HPC ecosystem within a competitive timeframe.

EU Plans for More Computing Power

As its use has become more common, HPC has become a priority issue for most EU Member States in recent years, and with it an attempt to address the limits of Europe's computing power. The need became more pressing from 2015 onward, after both U.S. and China developed their plans for HPC. There was thus pressure in the EU to aim for exascale computers too, and to make the EU space not only a consumer but also a producer of computing power. Within the EU, too, Thierry Breton, the current EU Commissioner for Industry, then CEO of Atos, strongly supported the initiative. The result has been new HPC initiatives and funding at a European scale, as part of a broader agenda for European digital infrastructures.

Two initiatives in the EU are ongoing: a plan to build supercomputers in the EU, including exascale HPC, known as the EuroHPC Joint Undertaking (JU), and a plan to develop an EU microprocessor for extreme-scale computing, known as European Processor Initiative (EPI). In 2017, seven EU member states—Germany, Portugal, France, Spain, Italy, Luxembourg, and the Netherlands—signed a declaration establishing the EuroHPC Joint Undertaking. The legal and funding entity was established in 2018. The EU Commission's DG Connect did a lot of the initial work, before EuroHPC became autonomous in September 2020. In the meantime, two private actors (the Big Data Value association, and ETP4HPC) joined the public-private partnership, as well as several non-EU countries, including Norway and Turkey (but not the UK)—reaching 33 members.

The principle is one of co-funding between the EU, its member states, and private actors federated in an association. Participating countries and entities coordinate their efforts and pool their resources. During the initial phase of 2019-2021, the JU had a €1 billion budget. On July 13, 2021, the European Council adopted a regulation on establishing the EuroHPC, thus allowing existing activities to continue. The new regulation will grow the initiative's budget, staffing, and missions. EuroHPC funding for 2021-2027 (to be matched by participating states) will come from Digital Europe (€2 billion), Horizon Europe (€900 million), and the Connecting Europe facility (€200 million).

The funding will be used toward advancing a dual goal: to deploy top-of-the-range supercomputing infrastructure across Europe to match users' needs, and to develop a research and innovation ecosystem for HPC technologies in Europe. The JU aims to deploy two exascale machines by 2023, which France and Germany are hoping to host. In France, the partnership between the CEA and Atos-Bull, via the GENCI, is driving the progress toward exascale, and the post-*TERA 1000* machine. In November 2020, they chose to integrate Fujitsu's A64FX processor technology, the same that equips the *Fugaku*, to develop the first French exascale computer.

Before exascale machines are built, eight hosting entities, around Europe, have been selected to host five petascale and three pre-exascale machines. Each of the five petascale machines will be worth between €12 million and €30 million each. The first computer, the Atos-built *Vega*, was inaugurated in March 2021 in Slovenia.

The EU's plan also includes three pre-exascale machines (at 10^{17} flop/s). Two are currently under construction: one, LUMI in Finland (Cray-HPE, with AMD CPUs and GPUs); and the second, Leonardo, in Italy (Atos-built with Nvidia GPUs), respectively worth €144 million and €120 million. The third one, MareNostrum 5, will be located at the Barcelona Supercomputing Center, but its procurement is currently in limbo. In this case, the shared

desire to procure petascale or exascale machines to respond to users' needs conflicts with another goal, which is to support and develop European industrial capabilities in HPC.

Two bids competed for winning the procurement contract: a U.S.-Chinese consortium with IBM and Lenovo, and Atos. The initial technical evaluation showed that IBM and Lenovo offered a more powerful machine at a better price. Atos' advantage, by contrast, was to have a supply chain that is more embedded in Europe—so one question was whether the latter should be a defining criterion in favor of choosing Atos. The EuroHPC criterion of "EU added value" does include an evaluation of how much a bid "reinforce[s] the digital technology supply chain in the Union." In light of this requirement, the EuroHPC advisory board recommended opting for the Atos offer: a choice which France supported, but Spain opposed. The issue became so political as to be the object of a discussion between the Spanish Prime Minister Pedro Sanchez and the French President Emmanuel Macron in March 2021. In May 2021, EuroHPC cancelled the tender, under the justification that the COVID-19 pandemic had changed the specifications required for the machine.

Energy consumption is becoming a major issue for the expansion of computing power and of the data economy. The huge increase in computing power and energy is in large part attributable to the training of machine learning programs. Aside from environmental considerations, this also has economic costs.

Energy Efficiency & Tech Sovereignty

Access time to EuroHPC machines will be allocated to European scientific, industrial, and public sector users in such way that it maximizes the positive impact of these systems on Research and Innovation (R&I). Indeed, the second goal of EuroHPC, parallel to infrastructure deployment, is to develop an R&I ecosystem for HPC in Europe that includes hardware and software capabilities, applications, training, and skills. That ecosystem, in turn, should contribute to Europe's double agenda: the Green Deal and technological sovereignty.

Energy consumption is becoming a major issue for the expansion of computing power and of the data economy. The huge increase in computing power and energy is in large part attributable to the training of machine learning programs. Aside from environmental considerations, this also has economic costs. The electricity bill for a supercomputer amounts to tens of millions of euros per year. The *Fugaku* consumes 30 to 40 megawatts, with a corresponding yearly cost of up to €40 million per year. For a country like France, the limitation to the deployment of an exascale machine is not so much technical as financial. In France, the current budget allocated to HPC only permits to consume half of that energy.

As part of Europe's Green Deal, any plan to develop HPC in Europe has to address the question of energy efficiency. Europe is already well positioned in the Green500 ranking, another ranking by Top500 that looks at power efficiency (in GFlops/Watt) in supercomputers: there are four Atos-Bull machines in the top 10, which is better than in the regular ranking where only one Atos-Bull machine makes in to the top 10. The EU intends to continue down this path. As part of EuroHPC, the laboratories that apply for hosting machines must be exemplary in terms of energy-efficiency. For instance, the LUMI, which is being installed in Finland, will be powered by hydropower from a nearby river.

Europe's two agendas of the Green Deal and technological sovereignty are coming together when it comes to processors: not only do processors play a big role in defining the power efficiency of a machine, but the past couple of years have also showed that foreign dependences on such technology causes risks of disruption.

The project for European low-power microprocessors—known as European Processor Initiative (EPI)—was launched in 2015 and started in practical terms in 2018. It gathers 28 public and private partners, including the CEA, STMicroelectronics, BMW, and various universities and research labs, and is coordinated by Atos. The EPI will create advanced processors for HPC applications. The main guidelines for a first generation of processors were announced in June 2019, and this vision was further materialized with the operational launch of SiPearl, a start-up company responsible for the design of the chips. A first prototype of processor, Rhea (which is largely based on a design by the British company ARM) was presented in January 2020. SiPearl hopes to launch Rhea in 2022 and to deliver it on time for the European exascale supercomputers in 2023. Aside from supercomputers, SiPearl aims to develop other microprocessors for other, bigger markets like autonomous vehicles, edge computing, and data centers.

The EPI's processors aim to be extremely energy-efficient: SiPearl promises it will halve the energy consumption of supercomputers. In principle, they also aim to fill a political and strategic goal, as they are "proudly designed in Europe to set out Europe's

technological sovereignty." Yet, at this point, the enterprise is faced with a lack of investment: presently the HPC sector is largely financed by national or European budgets and grants, but private investment is missing to make it viable. Finally, it is worth noting that the processors will indeed be *designed* in Europe, but the chips will most likely be manufactured by TSMC.

Quantum Computing's Revolution

According to Moore's Law, computing power doubles every two years, as the number of transistors on integrated circuits doubles. This trend is facilitated by the gradual reduction in the size of semiconductors, together with other advancements in digital electronics. However, we now frequently read that we are reaching the end of that law, as we are close to reaching the physical limits of nanoscale computer chips. According to a 2018 report by the European Investment Bank, "by 2025, hardware configurations could come to the end of exponential capacity increase" of classical computers.

In contrast to these physical limitations faced in classical computers, quantum computing exploits the characteristics of quantum physics and promises to multiply computing power exponentially. Consequently, quantum computing has become a strategic field in which governments, research laboratories, technology companies are increasingly investing, with a view to reaping the benefits of the quantum advantage.

Quantum information sciences emerge from the consideration that quantum physics (i.e., physics at the atomic or sub-atomic level) has implications for how systems like computers process information. In turn, quantum effects can be leveraged for computing information. Quantum computing is one segment of the field of quantum information sciences, which is vast and also includes communication and cryptography, metrology and sensing, and simulation, with wide-ranging application domains. Quantum information technologies currently stand at various levels of readiness. Compared to sensing and cybersecurity applications, quantum computing is the furthest away from market readiness, but it also has the highest disruption potential.

Explanation of Its Principles

Quantum computing emerged recently, and its development has accelerated in recent years. In 1995, scientists understood that quantum algorithms will make it possible to perform calculations in record time, and that this posed security challenges for information systems. The following year, IBM proposed the first principles of the quantum computer and introduced the first 2-quantum bits (qubit) computer. Five years later, in 2001, IBM researchers managed to factor the number 15 using quantum bits.

Quantum computers, as they exploit the special properties of matter in quantum mechanics, constitute a whole new paradigm in computing—whether in terms of hardware or software. In classical computing, the bit is the basic unit for storing information. Its value is either 1 or 0. In quantum computing, rather counter-intuitively, the basic unit, the qubit, can be "more or less 0" and "more or less 1," in varying proportions. This superposition of states allows for the multiplying effects of quantum computers compared to classical ones: where a classical computer can provide a result of a calculation at the end of a chain of successive instructions, qubits allow 2^N simultaneous combinations and provide an instantaneous solution at the time of measurement (however, without indication of the process). Consequently, quantum machines allow certain computations to be performed exponentially more quickly than by classical computers.

Quantum computers, as they exploit the special properties of matter in quantum mechanics, constitute a whole new paradigm in computing—whether in terms of hardware or software.

To exploit the properties of quantum physics, a quantum computer manipulates the states of particles using lasers or electric and magnetic fields. Different quantum processor technologies are currently undergoing experimentation in quantum research laboratories. Most industrial teams, including IBM and Google, as well as the UK in collaboration with California-based Rigetti, have focused on qubits as superconducting circuits that are cooled to extreme temperatures close to absolute zero, where certain materials conduct electricity with no resistance. They are the qubit technologies that appear to be the most advanced.

"Trapped-ions" is another technology that is also very promising. These are electrically charged atoms (ions) that are cooled and "trapped" with lasers. This technology is pursued by Honeywell, IonQ (sponsored by the United Arab Emirates with the University of Maryland) and the EU Quantum Flagship project "AQTION." Photon-based technologies are also being developed, not least by China's University of Science and Technology. Finally, the emergence of quantum computing goes hand in hand with technological advances in many scientific and technological fields: nanotechnologies, cryogenics, materials sciences, lasers, etc.

It is unclear today which qubit technology or technologies will eventually prevail. Currently, governments, technology

companies, and investors need to adopt a "Darwinian" mindset: even if still at an experimental stage, it would be risky to bet on the failure of quantum computers or to choose one technology over another. Eventually, there are probably going to be different types of quantum computing systems that will coexist.

Remaining Challenges

The American physicist John Preskill developed the concept of "quantum supremacy," which will be attained when a quantum machine solves a mathematical problem that no classical computer can solve due to the latter's physical limitations. Examples of such limitations include a calculation that would require millions of years to solve, or a calculation that would require more particles than there are in the universe.

What remains unknown at present is both how and when the industry will reach the point where a quantum computer can solve a relevant problem faster than a classical computer for concrete commercial applications. We are currently at the same point in the development of quantum computing as were scientists in the 1950s, when conventional computers ran on vacuum tubes.

Some U.S. and Chinese laboratories have successfully set out on a race for "quantum supremacy," as I will discuss below. However, most governments, research labs and start-ups around the globe are seeking to harness "quantum advantage," and to develop practical uses of quantum computing. Quantum advantage will come down to combining a quantum machine with a classical machine to reach a level of acceleration of computing that is sufficiently significant to provide an advantage compared to classical machines. What remains unknown at present is both how and when the industry will reach the point where a quantum computer can solve a relevant problem faster than a classical computer for concrete commercial applications.

According to the U.S. Department of Energy, we are currently at the same point in the development of quantum computing as were scientists in the 1950s, when conventional computers ran on vacuum tubes. The technologies behind classical computers are today sufficiently performant to create, transfer, store information with a reliability rate close to 100 percent, and few resources (memory, CPU) are needed to correct errors that inevitably result from electronic components.

We are far from there with quantum computers: they remain extremely sensitive to interactions with their environment, which affects the properties of quantum bits and the quality of the output. The mere day-to-day vibrations of a building in which a quantum machine is located can lead qubits to "decohere" and lose their programmed quantum information. Quantum hardware requires intricate wiring to control and measure qubits and this also introduces noise, in a way that increases as the number of qubits grows. Thus, a key challenge is to solve the noise and errors caused by the fragility of quantum systems. Noise-correction, though adaptations in code, algorithms or hardware is thus a central workstream of quantum research.

The "Holy Grail" of quantum computing science—which would constitute a real game-changer—would be the advent of large-scale, general-purpose quantum computers (known as LSQs).

Today, Noisy Intermediate-Scale Quantum computers (NISQ) are a first generation of quantum computers that are not so precise, but which can demonstrate the validity of technologies and algorithms. They provide experimentation grounds to identify use cases and develop quantum algorithms. Practical uses will come later. NISQs contain between around 50 to a few hundred qubits. Below 40 qubits, a classical computer can be faster than a quantum one; above 60 qubits, a quantum computer is always faster.

It is estimated that a quantum computer with 1,000 to 5,000 qubits will start having real-world applications, and implications for cybersecurity. But the "Holy Grail" of quantum computing science—which would constitute a real game-changer—would be the advent of large-scale, general-purpose quantum computers (known as LSQs). But their arrival is uncertain.

If some, like Google, have already succeeded in performing quantum calculations which demonstrated quantum supremacy, the error rate is so high that we are still very far from achieving the promises of quantum computing. Today, the best qubits make a mistake every 1,000 operations—that is, 10 billion more errors than a classical computer. Thus, most experts argue that to have an efficient error correction rate, these computers would need to have millions of qubits.

This presents another problem, which is space: today, an experimental quantum computer of a few dozen qubits occupies a full room, not least due to refrigeration and shielding requirements. Another option is to develop a qubit technology that can limit or correct errors. In either case, it is necessary to develop qubit technology that can be manufactured at scale.

Two other necessary lines of effort are classical-quantum computers integration, and software design. Quantum computers will not operate independently but, instead, for the foreseeable future, will work in conjunction with classical computers. A classical computer will be able to do bulk information management and data processing, while the quantum part of the machine could solve a specific problem.

The realization of hybrid machines that integrate quantum and classical computers still pose many engineering challenges from both a software and a hardware point of view.

The realization of hybrid machines that integrate quantum and classical computers still pose many engineering challenges from both a software and a hardware point of view. When it comes to software, companies are today designing software that runs on classical supercomputers that mimic perfect quantum computers, as well as quantum computer emulators. However, practical considerations severely limit the circuit sizes which can be emulated. Due to the laws of quantum physics, a classical computer can only simulate a quantum computer of up to around 40 qubits. Nonetheless, simulators and emulators are useful to help researchers experiment with quantum systems and to develop algorithms that can make use of the peculiarities of quantum computers as well as their future applications.

Applications and Implications

Conscious of the step-change that will come when quantum machines are ready, both industries and governments are examining the practical use cases of the intermediate devices that will likely be available within a decade.

To begin with, quantum machines will speed up the development of AI, as they will allow acceleration of deep learning and neural networks, with both civilian and military applications. In the military domain, for instance, quantum AI could facilitate the development of autonomous weapon systems, and accurate intelligence, especially when coupled with other quantum technologies.

In addition to AI, quantum computers will be especially suited for tasks of factorization, optimization, and simulation. Factorization is especially relevant for cryptography and makes the cybersecurity implications of future large-scale quantum computers a major concern for states. In 2015, the U.S. National Security Agency (NSA) updated its encryption system to make it "quantum resistant." While significant advances in quantum computing are still required to break current encryption methods, a fully functioning quantum computer could allow a country or a non-state actor to break any public encryption key that is secured with current technology. That includes the RSA, the cryptosystem currently used to secure online payments. According to some estimates, it would take a classical computer 300 trillion years to crack an RSA encryption key (of 2,048 bits), while a quantum computer with 4,000 stable qubits could in theory do the same in just ten seconds. Conversely, quantum technology can also be used to secure communications.

A fully functioning quantum computer could allow a country or a non-state actor to break any public encryption key that is secured with current technology.

Complex simulation will arguably form a key part of the uses of quantum computers. The simulation of molecules requires a lot of computing power, as the bonds and interactions among atoms behave probabilistically, which exhausts classical computing logic. One quantum scientist was recently quoted as saying, in this context, that quantum computing is about "simulating nature, using the laws of nature." Simulation at the molecular scale could have applications in medicine (e.g., for creating targeted medicines), in energy (e.g., more efficient batteries), in sustainable agriculture (e.g., fertilizers), or even for developing processes to capture CO_2 present in the atmosphere.

Finally, quantum computers would be very useful for optimization tasks required for autonomous vehicles. With a fully autonomous fleet, it should theoretically be possible to optimize the individual journey of each vehicle according to its place of departure and destination. Conventional algorithms could work with a limited quantity of vehicles, but beyond a few hundred vehicles and journeys, traditional calculation capacities would be largely saturated. Optimization is also key for actors in the energy sector in the development of electrical networks and the management of electricity consumption in the context of a multiplication of electric vehicles.

Considering the enormous scientific and technological uncertainties that remain, the full business implications of quantum technologies will unfold and sediment over time. According to a report by Boston Consulting Group, we should expect quantum computing to develop toward maturity over three generations spanning the next 25 years. It is likely that ad hoc civilian uses of quantum machines will develop over the next 10 to 15 years, and that a quantum computer capable of breaking current encryption methods will see the light by 2040.

In any case, quantum computers will not replace conventional computers. They will likely be complex and fragile machines with much narrower functions than universal classical computers, and they will thus be rare: at least at first, only a few machines will exist and be accessible on the cloud. Given the complexity of the field of quantum technologies, delegating them to providers on a cloud would avoid companies being forced to develop extremely advanced skills that are difficult to acquire. Thus, quantum computers will not become a replacement but a complement to current HPC tools.

Considering the enormous scientific and technological uncertainties that remain, the full business implications of quantum technologies will unfold and sediment over time we should expect quantum computing to develop toward maturity over three generations spanning the next 25 years.

Despite these limitations, quantum computing will have significant business and financial implications. The Boston Consulting Group sees a potential addressable quantum computing market of £4 billion (€4.7 billion) by 2024. In a slightly less optimistic scenario, the Quantum Economic Development Consortium and Hyperion Research foresee a 27 percent yearly growth from 2020 onward, with a global market worth $830 million (€701 million) by 2024.

EUROPE IN THE QUANTUM RACE

The 2010s saw a clear acceleration of global competition around quantum information processing technologies. Illustratively, while in 2014, the UK Ministry of Defense judged the field of quantum information processing as "too immature" for near-term defense and security application, the UK Defense Science and Technology Laboratory (DSTL) reported in June 2020 that "the progress achieved both nationally and globally has exceeded early expectations," so that today "many regard the rush to develop quantum computing as a new 'space race.'"

Quantum computing has become a race not least because of the risks of lagging behind. A first risk is cybersecurity, as explained above, as quantum computers will be able to break current encryption protocols in seconds. Another risk is access to technologies. Quantum cryptography and quantum computers indeed are making their way onto defense and strategic goods lists, and are thus becoming subject to export restrictions. The enabling technologies that are needed to make quantum computers work can also be placed under control: certain qubits require extremely cold temperatures that are obtained thanks to cryostats, a technology whose export to China the United States is considering blocking.

U.S.-CHINA COMPETITION AND QUANTUM TECHNOLOGIES

Currently, the most advanced countries in the field for quantum computing, in terms of technological advancement and government strategy and funding, are the United States and China—they have each already claimed quantum supremacy—as well as a few EU member states (e.g., France, Germany, and the Netherlands) plus the UK.

The most advanced countries in the field for quantum computing, in terms of technological advancement and government strategy and funding, are the United States and China.

Washington's concerns of being overtaken by China have grown since Beijing demonstrated its capacity in satellite-based quantum communications in 2017. In 2018, President Donald Trump launched the National Quantum Initiative, with $1.2 billion (€1 billion) in public funding for an initial period of 5 years, until 2023. Trump set up a National Quantum Coordination office within the White House, and in August 2020, the U.S. launched its national quantum research centers, and an additional $237 million (€200 million) was voted as part of the 2021 budget. The United States Innovation and Competition Act (USICA), approved by the U.S. Senate in early June 2021 (it has not yet been taken up by the U.S. House of Representatives), proposes to allocate $150 billion (€128 billion) between 2022 and 2026 for research, innovation, and education in critical and emerging technologies, including quantum technologies.

Aside from the government, big technology firms are pouring huge amounts of money into their own research in quantum science—although their internal investment figures are not disclosed. The financial power of private investors and the attractiveness of large digital companies like IBM, Google, and Intel have given those companies a head start in quantum research. It was IBM that proposed the first principles of a quantum computer and introduced the first two-qubit computer. By 2016, the company had managed to simulate a molecular structure and reached the theoretical threshold of quantum supremacy with 50 qubits. The following year, Intel unveiled a 49-qubit calculator, and Google a 72-qubit processor. In September 2019, Google claimed to have achieved quantum supremacy with a 53-qubit quantum computer using superconductors. It succeeded in completing in just over three minutes a calculation that Google said would take

10,000 years to solve by a conventional supercomputer. IBM downplayed this achievement as it affirmed the calculation would take only 2.5 days on the most powerful of supercomputers.

Since 2016, IBM has offered an online quantum programming interface, IBM Quantum Experience. This platform offers a quantum programming simulator that gives access to 22 IBM computers. To date, more than 325,000 users have registered with it and more than 700 articles have been published based on work carried out on this machine. Aside from IBM, other American companies like Microsoft, Amazon, and Rigetti, as well as Canada's Xanadu, offer online services of small-scale quantum computing chipsets with capacities of up to 65 qubits. When it comes to on-premises machines, U.S. companies, starting with IBM, have already built and exported quantum computer prototypes. IBM's strategy is to make its technology available online, so as to encourage early adoption of its product. It has exported the first ever commercial quantum computer (albeit still experimental), the 20-qubit Quantum System One, to Germany and Japan, to drive quantum R&D there. And it is currently working towards making a stable quantum computer capable of handling more than 1,000 qubits by 2023.

While estimates of China's actual spending on quantum research vary, the country is leading in terms of patent holding in quantum communication and cryptography hardware as well as software.

Meanwhile in China, efforts have been ongoing since 2015, after the 2013 Snowden revelations prompted anxiety over the extent of U.S. intelligence capabilities and activities and intensified the government's focus on quantum communications and computing. Beijing has thus sought to leverage quantum networks to secure China's most sensitive communications. Simultaneously with Obama's plan entering the field, Beijing listed quantum as a part of China's major science and technology priorities to be developed by 2030.

There is limited information about total funding on quantum technologies in China. Officially, China spent over $302 million on quantum sciences between 2013 and 2015. In 2017, Beijing announced a $10 billion investment into a new quantum computing research center. While estimates of China's actual spending on quantum research vary, the country is leading in terms of patent holding in quantum communication and cryptography hardware as well as software.

Robust research has led to rapid progress and even leadership in other quantum technologies (cryptography and communications), as was illustrated when China launched the world's first quantum communication satellite in 2016. When it comes to quantum computers, China's efforts have been more recent, but Beijing has been quick to catch up. In December 2020, a group of researchers from the University of Science and Technology of China (USTC) made a credible claim to have achieved quantum supremacy, using a photonic system to complete a calculation in 200 seconds that would have taken a supercomputer 2.5 billion years. That is to say that the calculation was performed 100 trillion times faster than with a classical supercomputer. In June 2021, China again demonstrated quantum advantage, this time with a system based on superconducting circuits.

Europe's Growing Quantum Ecosystem

There are serious players in quantum technologies in Europe, among which is the UK. The head of the Government Communications Headquarters (GCHQ) suggested in April 2021 that the UK must develop "sovereign capabilities" in quantum computing, not least to respond to the cyber threat posed by China. The country is not starting from scratch—far from it, in fact: it launched its National Quantum Technologies program as early as 2013. The British government planned to invest £400 million (€467 million) in the first phase (2014-2019) and £350 (€400 million) in the second. In the past year, the UK government has renewed its commitment to quantum and other information technologies in a series of policy documents and decisions. The March 2021 *Integrated Review*—the main document guiding the UK's foreign, security, and defense policy in the post-Brexit context—placed a strong emphasis on technological power and suggested the UK should be a leader in cyber technologies (quantum technologies included) and in new forms of data transmission.

Like in the U.S., new research centers and policy strategy positions are being set up in the UK. In June 2021, Boris Johnson announced he would create a National Science and Technology Council, chaired by the Prime Minister, as well as a new Office for Science and Technology Strategy, based in the Cabinet Office, and a new role of National Technology Adviser. A new National Quantum Computing Centre is being set up and will open in 2023. In September 2020, the UK government passed a £10 million (€11.7 million) agreement with U.S.-based company Rigetti to build the UK's first commercially available quantum computer. The UK also has homegrown companies. Meanwhile, in July 2021, Oxford Quantum Circuits (OQC), a UK-based start-up, announced that the company has launched the nation's first commercial "quantum computing-as-a-service" built entirely using its proprietary technology. OQC did not disclose how many qubits its machine

contains, but in 2017 the company was working on a 9-qubit system.

The German government is also investing in quantum technologies. An investment of €2 billion over five years was announced in June 2020 as part of a major stimulus injection, which builds on an initial government effort of €650 million for the period 2018-2022. One must add to this the contribution of Länders, including for example Bavaria's recent €300 million investment in a "Quantum Valley."

In June 2021, Germany's then-Chancellor Angela Merkel reflected on the fact that quantum computing can play a key role in the country's endeavor to "acquire technological and digital sovereignty," as Germany and the EU find themselves in the context of a "very intense competition." Merkel indicated a hope in promoting the development and production of quantum technologies in Germany to form a new industrial pillar, both in terms of hardware and software. First steps have already been taken: the construction of at least two quantum computers in Germany have been commissioned. The first machine was unveiled at the Fraunhofer institute for applied research, near Stuttgart, in June 2021. It is an IBM, the Quantum System One computer, the first of its type in Europe which was installed near Stuttgart, in June 2021. This will allow German researchers to work more intensively on future quantum applications. The choice of an IBM machine (and the cloud that comes with it) was justified by the fact that there are, currently, few leading European quantum companies. In the first step of its quantum computing strategy, Germany has been more focused on developing uses of quantum technologies than on supporting national quantum hardware companies.

In the first step of its quantum computing strategy, Germany has been more focused on developing uses of quantum technologies than on supporting national quantum hardware companies.

In February 2021, Emmanuel Macron unveiled a National Plan for Quantum Technologies that aims to make France the third-largest spender in the world on quantum technologies, behind the U.S. and Germany. The French plan has been in preparation since 2018, after Thierry Breton, then the CEO of Atos, called on the French government to elaborate a quantum strategy. At the time, he was one of the few French industrialists to be vocal on the issue. The French plan for quantum technologies was announced in February 2021. It calls for a total of €1.8 billion public-private investment (including €1 billion public funding) between 2021 and 2025, going toward education and training, research, support for start-ups, and support for industrial deployment and innovation.

With the strategy, France's goal is to master decisive quantum technologies, including quantum accelerators, simulators and computers, business software for quantum computing, sensors, and communication systems. The bulk of the funding will go to quantum computing, with NISQ and LSQ totaling €784 million.

The choice of which qubit technology to favor is based on an analysis of the chances of success of a given technological avenue, the presence of a critical mass of researchers in France, and the presence of an industrial base able to build the technologies. Trapped ion technologies—developed by Honeywell, IonQ, and AQT (Austria), for example—are considered very promising but difficult to develop in France due to a lack of a critical mass of researchers. In the context of limited funding, the objective is to gradually diminish risks, but for the time being, France is treating all technological avenues equally.

The French 2021 Quantum Plan draws lessons from the past failures at government planning, that is to say large, national investments in certain strategic sectors and infrastructure. According to Mathieu Landon, in charge of industry in the French Prime Minister's office, one lesson learned is that such state strategies must be based on ecosystems, where there are already research and industry, rather than building an ecosystem from scratch. The French quantum ecosystem is already rich. It builds on research institutions (the CNRS, especially Paris-Saclay University, the CEA, and INRIA) as well as large companies involved in quantum computers (Atos) and telecommunications (Orange and Thales), and quantum-relevant enabling technologies, such as cryogenics (Air Liquide).

Atos has become involved in quantum simulation and testing algorithms for future quantum computers. In 2017, it started commercializing the Atos Quantum Learning Machine, a quantum computer simulator, capable of processing up to 30 qubits in memory. Atos delivered simulators to the Oak Ridge National Laboratory, which is part of the United States Department of Energy (DOE), to the Argonne National Laboratory in the United States, to the CEA, and to the Hartree Center, a British research laboratory.

Aside from large companies, over recent years, France has seen its quantum start-ups flourish. Of the world's 260 quantum technology start-ups and SMEs, almost 10 percent are thought to be in France. Pasqal is a hardware quantum company, created in 2019 which is developing a quantum computer based on atoms manipulated by lasers, intended for high-performance computing centers. It is backed by the Optics Institute of the University of Paris-Saclay. The company has so far built a quantum machine that works on its premises, and it has also received an order for two other machines to

be delivered early 2023 to the GENCI in France and to the German research center in Jülich. The start-up has already also entered partnerships with Atos and Crédit Agricole. Pasqal has also decided to make their computer available on a cloud.

Alice & Bob is another promising start-up. It was created in February 2020 as a spin-off of an ENS-INRIA team. It raised €3 million a few months later from French funds Elaia Partners and Breega. The "cat qubit" is a groundbreaking discovery on self-correcting qubits that led to the creation of the start-up. According to a May 2020 item in a leading trade publication, the start-up is aiming to create an error-free, or "ideal" quantum computer, "which is one of the fundamental scientific problems that has limited development of more powerful quantum computing." It plans to deploy the world's first ideal quantum processor in the cloud by 2026. Amazon is seeking develop a quantum computer on the basis of this very technology, following scientific publications on self-correcting qubits. While this is testament to the relevance and excellence of their discovery, it places Alice & Bob in competition with a tech giant that has incomparable financial room for maneuver and scientific teams that are ten to twenty times larger than those of the French start-up.

Aside from large companies, over recent years, France has seen its quantum start-ups flourish. Of the world's 260 quantum technology start-ups and SMEs, almost 10 percent are thought to be in France.

When Science Becomes Strategic Technology

International collaboration is central to scientific research and vital for Europe to reach the scale necessary to compete globally in quantum technologies. Since 2018, the EU too has made quantum technologies a priority and has committed €1bn to co-finance collaborative research programs over 10 years. The Quantum Flagship is one of the EU's largest and most ambitious research initiatives. In fact, it is currently the largest international funding framework for quantum technology. It brings together research institutions, academia, industry, enterprises, and policymakers in a joint and collaborative initiative on an unprecedented scale.

Among the funded programs are a quantum computer (accelerator) based on trapped ions ("AQTION," based at the University of Innsbruck) and a quantum simulation platform ("PASQuanS," carried out at the Max Planck Institute in Munich). Atos leads both projects, on the industry side. The EU is also funding projects in other quantum technologies, especially quantum communications. Bilateral collaborations among EU member states are also developing—partly motivated by the goal of securing EU funding—as illustrated most recently by the signing of a Memorandum of Understanding between France and the Netherlands, for academic cooperation, but also to build synergies between French and Dutch companies and create quantum unicorns.

The transition of quantum sciences from the realm of academia to concrete applications with security and industrial applications has been creating new dilemmas for the EU's collaborative projects and cooperation with non-EU members. The UK, as explained above, but also Switzerland and Israel have significant quantum research ecosystems and are willing to join the EU's Horizon Europe programs in quantum and space.

The transition of quantum sciences from the realm of academia to concrete applications with security and industrial applications has been creating new dilemmas for the EU's collaborative projects and cooperation with non-EU members.

The EU Commission, and in particular Thierry Breton, has opposed the participation of several non-EU countries, (including the aforementioned three states) in EU research programs on quantum computing, saying the goal is to "make independent European capacities in developing and producing quantum computing technologies of strategic importance," with applications in security and dual-use technologies. However, a group of EU countries, led by Germany, pushed to maintain the openness to Associated Countries in quantum and space research programs, arguing that the bid for technological sovereignty should not get in the way of scientific collaboration.

The Global Race Is Also One for Capital

While it has yet to reach the volume and quantity of other industries like artificial intelligence, the ecosystem of quantum technology companies, especially start-ups, continues to grow around the world. Some estimate that there are over 260 quantum technology startups and SMEs globally. Many start-ups are still at the stage of applied research and sometimes still fundamental research, and quantum computing remains an uncertain technological sector.

Investment is at the heart of the matter. As suggested above, funding is key for allowing researchers to conduct their experiments, but also for scaling up and commercializing quantum systems. Besides, if, as mentioned above, future import restrictions on quantum technologies are feared, foreign takeovers of successful companies are too. Private sector investment is needed, if France and the

rest of the EU are to retain their talents and prevent individual researchers and promising start-ups from going overseas. Globally, the private sector's involvement in the funding of quantum start-ups has boomed: quantum-computing companies landed $779.3 million (€662 million) in 77 deals in 2020, a surge from $288.3 million (€194 million) in 69 deals in 2019. Several quantum technology start-ups are now valued at several hundred million euros and at least two are now publicly traded.

While it has yet to reach the volume and quantity of other industries like artificial intelligence, the ecosystem of quantum technology companies, especially start-ups, continues to grow around the world.

The current investment boom in quantum start-ups is so far playing into the hands of American venture capital funds and large digital companies. The Canadian firm Xanadu, too, raised $100 million (€85 million) largely from U.S. investors, including the CIA's investment branch, In-Q-Tel. In the UK, the leading British start-up PsiQuantum was established in 2016, but has since settled in California. It is promising to build a one-million qubit large-scale, general purpose quantum computer by 2025. The move to the Silicon Valley was partly motivated by a need to raise capital. PsiQuantum has, so far, successfully raised a total of $665 million (€565 million) including, in late July 2021, $450 million (€382 million) from mostly U.S. investors such as BlackRock and Microsoft's venture fund, M12. The story recalls that of DeepMind, the British AI company that Google acquired for £400 million (€628 million) in 2014. The UK government has taken action on the issue, when in July 2021, it set up a new fund for R&D intensive firms, including quantum companies. To be eligible, businesses must have secured funding commitments from private investors venture capitalists.

All countries that get into the quantum race but have limited private investment face the same risks as UK companies. This is especially true for EU-based companies, where venture capital is scarce. Quantonation is a Paris-based investment fund — the first in the world that is specialized in quantum technologies. It was set up in late 2018, and funded Pasqal in 2019. Quantonation supports quantum companies in their early stages, but for later stages, other investment funds must take over and invest hundreds of millions to help seeded companies grow. This is where there is a risk for EU companies that seek to commercialize products, and there is a real challenge for ensuring not only that companies are not taken over by foreign capital, but also that they can grow in the European Union space.

TRULY STRATEGIC OPPORTUNITIES

The democratization of high-performance computing and new levels of conventional computing power, together with the emergence of disruptive quantum information technologies, are changing the calculations of governments, researchers, and private companies alike. Private companies are finding new ways to use the potential of data analysis, governments are developing strategies to gain relative technological power and ensure the security of their digital systems, while scientists can hope to make new discoveries in medicine and in the fight against climate change. Technological progress is also promising to significantly reduce the energy consumption of computers, which has become a bigger concern as uses continue to grow.

All countries that get into the quantum race but have limited private investment face the same risks as UK companies. This is especially true for EU-based companies, where venture capital is scarce.

The global distribution of computing power is changing. While the U.S. has for long dominated the sector of conventional computing, not least with the defining role played by IBM, China's Lenovo has now become the first HPC company worldwide in terms of market share. Today, the U.S. and China are also neck and neck in the race for quantum computing, with massive investments and impressive technological achievements. These raise the risk of developing hardware-dependent tools and technology dependencies.

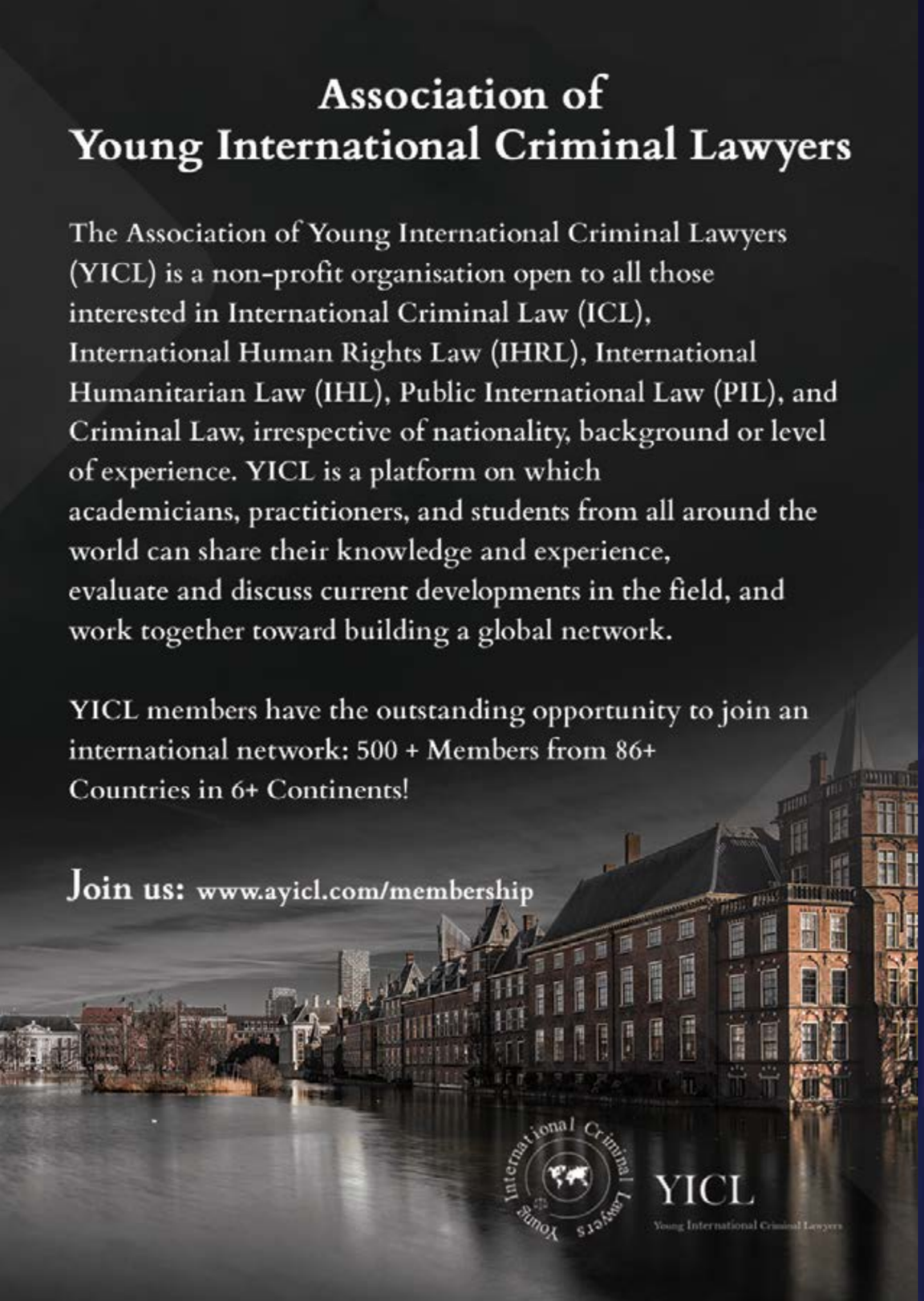
But the ongoing quantum revolution is nurturing a wealth of actors, from research laboratories to start-ups and investment funds, which could further redistribute computing power across the globe. Technologies with a lower level of readiness offer the EU and its member states a chance to position itself early in this emerging sector and develop capacities along the value chains of quantum computing in hardware and software. European governments, including France and Germany, as well as EU institutions, have made significant efforts in this direction. Together with private investors, they will need to remain committed throughout the life cycle of this emerging and highly disruptive technology.

Association of Young International Criminal Lawyers

The Association of Young International Criminal Lawyers (YICL) is a non-profit organisation open to all those interested in International Criminal Law (ICL), International Human Rights Law (IHRL), International Humanitarian Law (IHL), Public International Law (PIL), and Criminal Law, irrespective of nationality, background or level of experience. YICL is a platform on which academicians, practitioners, and students from all around the world can share their knowledge and experience, evaluate and discuss current developments in the field, and work together toward building a global network.

YICL members have the outstanding opportunity to join an international network: 500 + Members from 86+ Countries in 6+ Continents!

Join us: www.ayicl.com/membership



cirsd

CENTER FOR INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

Program on International Law

In a world characterized by a growing number of humanitarian crises, heightened insecurity, rising inequalities, and an increasing number of threats to international law, CIRSD remains committed to its mission of providing expert analysis and practical ideas for action.

With the aim to provide insight into the international legal system and promote better understanding of how international law comes to shape and affect global events, CIRSD has proudly launched a new Program on International Law.

Since its inception, the Program has featured views of legal experts on core topics associated with international law – Space law, International Criminal and Humanitarian Law, and Data Protection.

CIRSD encourages submissions from legal professionals and scholars to offer their own unique perspective. For more details, contact Ms. Ana Prokić - Director of the Program on International Law, via her email address: **ana.prokic@cirsd.org.**

Visit the Program page at:
cirsd.org/en/about-us/program/the-program-on-international-law

facebook.com/cirsd *linkedin.com/cirsd* *twitter | @cirsd*

CAN THE TRANSFER OF INTELLECTUAL PROPERTY SAVE THE WORLD?

Mohamed Jouan Salem AlDhaheri and John D'Agostino

IN recent years, the transfer of Intellectual Property (IP) has earned a bad name. Largely, this is due to growing tensions between the United States and China, a central theme of which has been American complaints regarding Chinese trade practices. More widely, however, globalization itself has gathered opposition, with many commentators increasingly doubting that an international economy is an obvious public good. And yet, IP transfer has the potential to transform regional economies, ameliorate fundamental human rights issues, meet climate challenges, and accelerate development—all to the ends of improved international relations.

So what is it to be?

This essay makes the case for trade. Specifically, it defends the simple (and now unfashionable) idea of international improvement through the transfer of IP. It argues that, in an era of capital and data flows (both of which are potential disruptors) there is every reason to harness and maximize the potentially stabilizing forces of other flows—in this case, the flow of ideas.

Moreover, the Middle East in general, and the United Arab Emirates (UAE) in particular, are the perfect testing ground for this thesis. Given its relatively high level of development, and its highly developed relationships with major economies in both the West and the East, UAE could become a regional super hub for IP—a bank of ideas and knowhow that brings forward regional development and rehabilitates the reputation of IP transfer. So doing might even go some way to saving the troubled reputation of globalization itself.

Mohamed Jouan Salem AlDhaheri *is Executive Chairman, CEO, and Co-founder of RainMKRS, an entrepreneurial catalyst whose mission is to bring together the world's leading companies, institutions, and entrepreneurs with the UAE's prominent stakeholders in the food and agriculture industry. You may follow him on Twitter @RainMkrs.* ***John D'Agostino*** *is Senior Advisor to Coinbase and lectures on Fintech at Columbia University. In 2020, he was named Chair of the UK Government's Asset Management Working Group in New York. You may follow him on Twitter @ johnjdagostino.*

COOPERATION AND COMPETITION

In his book *Skin in the Game: Hidden Asymmetries in Daily Life* (2018), Nassim Nicolas Taleb writes that "information does not like to be owned." He makes a good point. History is replete with examples of irrepressibly good ideas. In fact, it is founded on them. Early humans could hardly hide the discovery of fire or wheels, and it is central to the human story that this and other useful knowledge has always proliferated. Nor do modern humans act much differently. Everything from the jet engine and toothpaste to water wheels and iPhones will eventually find its way around the globe. In 1976, the popular British scientist Richard Dawkins coined a term to describe this sort of travelling idea: a "meme."

Will sharing commerce offer more developmental advantages than the disadvantages of losing one's own industrial secrets?

When it comes to economics, memes are, of course, a good thing. The creature comforts of modernity owe far more to commerce than they do the international political system. It is only to the good that ideas have a tendency to get around; but this is where things get complicated. Good ideas raise everyone's game. Very often, however, their authors are left impoverished. Hence the legal system attempts to incentivize commercial innovation with things like patents, status, and other rewards. Here's the point: if humans collaborate, humans also compete. Ideas can be exploited, even stolen. Sometimes people generate, from nothing, new ideas and make money. More often, they make money by commercializing or incrementally improving an existing idea. Cooperative efforts for the economic group as a whole can involve a zero-sum game for individuals.

These two contradictory behaviors—cooperation and competition—sum up human history. While cooperation is obvious on one level—technology, as we said, will find a way—competition is always present at another. Empires have risen, clashed, and fallen, all while balancing these two incessant forces: cooperation and competition. The result is that individuals, jurisdictions, and economies are never quite sure about exactly how open they should be.

The perennial question is therefore as follows: will sharing commerce offer

more developmental advantages than the disadvantages of losing one's own industrial secrets?

In other words, are the advantages of globalization still greater than its disadvantages? Is today's international economy a collective or individual zero-sum game?

A SEVENTH-DAY MOMENT

After the Cold War, the United States had re-made the world. And, when it rested and looked at what it had done, it saw that it was good. With the Soviet Union dissolved, the world was at last safe for democracy. Plus, as a nice little bonus, the world was safe for commerce too. The international community had a brief moment of thinking that—maybe, just maybe—the age-old dilemma of cooperation versus competition had been resolved. Competition has lost; cooperation had won.

The initial post-Cold War thesis of inevitable American influence preceded a second, newer idea. This second idea came after 9/11. It was the need to impose democracy and free markets primarily by military means, and not economic.

The 1990s were thus a heady time. Heralded as the beginning of a brand new international political economy, trade would be good, free trade better, and the eventual outcome of both—universal democracy—best of all. Having resisted the import of autocracy, America could now turn to the export of ideas. Human freedom would triumph, if not yet through the ballot box, then at least through the vanguard of trade. The jewel in this crown was, of course, the addition of China to the World Trade Organization (WTO), something finally achieved in December 2001. In November of the same year, then President George W. Bush had this to say of this development: "WTO membership […] will require China to strengthen the rule of law and introduce certain civil reforms. […] In the long run, an open, rules-based Chinese economy will be an important underpinning for Chinese democratic reforms."

Yet, at the turn of the century, Chinese democracy was not really on American minds. Instead, it was the terror attacks of September 2001 that commanded the gaze of the United States. Mobilizing its formidable military capacities in response to the destruction wrought in New York City and the Pentagon, the United States intervened, first in Afghanistan and then in Iraq. Primarily, these missions were national security operations. Enemies were fought and enemies were killed. But, over time, a combination of regime change and nation-building saw these interventions take on significant aspects of both economic development and humanitarian aid.

The result was two great and two very different models of superpower influence: economic and political sway, on the one hand, and the persuasive force of arms, on the other. The first, the model for American influence in China. The second, the model for American influence in the Middle East and Central Asia. That is not to say the two models cannot (and do not) work hand-in-hand. It is simply to point out that the initial post-Cold War thesis of inevitable American influence preceded a second, newer idea. This second idea came after 9/11. It was the need to impose democracy and free markets primarily by military means, and not economic.

The Trump Administration, in fact, originated many of the rolling Amerian complaints still in place today. And a centerpiece of his anger was the transfer of American IP abroad, particularly when that IP was transferred to China.

Today, in the early 2020s, it is clear the latter notion has seen a significant setback. The manner of American withdrawal from Afghanistan will lead to many commentators questioning future American interventions. But what of the first idea? Is there still hope for the concept of exporting economic development in the name of international cooperation?

TRADE SPATS AND IP

The above paragraphs rattled through some 30 years of global history at a breakneck pace. And they recounted a familiar story. This is the tale of Western euphoria in the early 1990s and how it gave way to Western angst in the pandemic-ridden 2020s. Unmentioned but obvious was the solidification of this angst, in 2016, with the election of Donald Trump to the U.S. presidency and his explicit renunciation of unrestrained global free trade. Trump, if nothing else, did not expect China to drift towards the democratic camp.

Today, we have a new administration. But it is important to study the Biden White House through the lends of Trump's. The Trump Administration, in fact, originated many of the rolling Amerian complaints still in place today. And a centerpiece of his anger was the transfer of American IP abroad, particularly when that IP was transferred to China. The Asian giant, it was felt in Trump's White House, had gained strategic prowess by (unfairly) gathering American knowhow. As we know, the result was a Sino-American trade spat—almost a trade war—that remains unresolved to this day. Trump, it seemed,

wanted to heed the advice of Napoleon and lull the Chinese back into their slumber. But, failing that, he would prod the Asian giant with his tariffs.

And yet, if considered, perhaps Trump's complaint should have been lodged with a previous occupant of the White House. Not so much with President Xi Jinping as with the aforementioned President George W. Bush. It was the Bush Administration that decided—focused on the war on terror as it was—to trust Beijing in the belief that opening up Chinese markets to American firms offered far greater gains than any potential downside. Even where those downsides might have included sharing certain American IP with domestic Chinese firms, the sheer size of the Chinese market was felt to outweigh any risks. Recall this was all back in the days of the Efficient Markets Hypothesis (EMH), and so on—a time before the 2007-2008 global financial crisis during which the power of markets was felt to be almost preternatural.

That is not, of course, how things played out. The twenty-first century relationship between the United States and China will be far more acrimonious. But, together, the two economies account for around 40 percent of global GDP. A complete separation would thus appear implausible. Moreover, each will continue to study the other. The implication is that at least some idea-sharing will continue. Put differently, the way the world economy functions suggests that ideas will still find their way around the global system.

If so, how can we maximize the benefits, especially locally?

If it is difficult to stop the flow of information, even between adversarial economies, why not attempt to enhance its benefits?

WATER, BREAD, AND SALT

There is an old saying, derived from U.S. constitutional jurisprudence, that the truth will win out in the marketplace of ideas. Applied to the information economy, so too will IP. Eventually, for better or worse, technology and its attendant ideas proliferate. If it is difficult to stop the flow of information, even between adversarial economies, why not attempt to enhance its benefits?

Alas, one of the more febrile political areas in the world is also one of the more prone to the political issues associated with a changing climate. The Middle East, in broad terms, will face some of the most acute climate-derived challenges of any region and yet is already facing some of the most fractured and complex regional political dramas.

There are obvious ways, however, in which the transfer of IP—particularly if managed through a regional hub—could promote the proliferation of new ideas and, with them, new outcomes.

Take water. One of the more, if not the most, disconcerting aspects of climate change will be a reduction in access to safe, clean, and affordable drinking water. While some regions will see increased rainfall, others will see increased drought. The irony is, of course, that the world is covered in water. Unfortunately, this water is ocean water: it is undrinkable and unsuitable for farming. This is particularly problematic for arid parts of the world. The UAE, for example, currently imports around 95 percent of its fresh produce. This, ultimately, is a product of a tightly restrained water supply.

In 1976 Chinese scientist Yuan Daoxian founded what was then the first Karst research center in China, the Institute of Karst Geology in Guilin. This institute eventually brought scientists together from all over the world to develop procurement and detoxification technologies for extracting potable water from limestone formation (i.e., the Karst in question). The offspring of this shared technological collaboration is now, many years later, the foundation for filling the supply gap of 5.5 billion cubic feet of water required for annual farming and human consumption needs in China. Sadly, this story is woefully underknown. This type of cross-border successes generally fades into obscurity even when responsible for extraordinary achievements. And yet, compare its quiet effectiveness against the very public media uproar in the United States over allegations of dangerous cooperation between America and China at the infamous Wuhan laboratory prior to the onset of the COVID-19 crisis. Once again, it is all too easy to see how very quickly the odds turn against technical cooperation.

But water remains key; and if extracting the essential element of life is one thing, using it effectively to power food production and commerce is quite another. This is to say that if technological cooperation stops at the most basic human level—i.e., sharing tech that supports only survival—the result will be insufficient. Sharing water alone will do nothing to reduce the structural causes of worsening economic inequality. We need also to share our wider economic fortunes; rich countries must embrace the need to share not just products, but also knowhow, with the poorer ones. Sadly, of course, cooperation between countries is not something for which the Middle East is famed, regardless of whether they are rich or poor.

This is where the UAE can step in. The ongoing normalization of relations

between the UAE and Israel is likely to produce a rapid progression in technology-sharing and cooperation in areas critical to combating ever higher temperatures and climate change, fighting against areas of aridity in water extraction and purification, and enhancing food production and food security. Were such information to be associated directly with Israel, such are the current realities of regional politics that much of it might be disrupted, even rejected. This is, of course, to no one's benefit, including far from an ideal outcome for Israel itself, which would benefit from a far more secure and stable neighborhood.

The Middle East in general, and the UAE in particular, are ripe for a grand experiment in the regional transfer of IP, a fast and hard push against the climate emergency and its attendant social and political fallout.

And what players would be required? They are threefold: first, private/public partnerships between governments (that will subsidize energy costs initially through fossil fuels as most projects transition to renewables); second, firms (that will look to build strong brands on the promise of localized food production); and third, academic institutions (that will see these new public/private ventures as perfect places for high-tech vocational training and empirical research on innovation). The UAE can offer all three, acting thereafter as the sort of regional ideas hub described above.

Ode to a Connected World

We need not forgo the long-term benefits of ideas, trade, and knowhow. As argued above, the Middle East in general, and the UAE in particular, are ripe for a grand experiment in the regional transfer of IP, a fast and hard push against the climate emergency and its attendant social and political fallout.

There are, perhaps, some elephants in the room, of which one is the American withdrawal from Afghanistan. Now Afghanistan is, of course, in Central Asia, not the Middle East. But it sits at the heart of the new Silk Road and its fortunes will invariably influence the countries lying to both its east and west. Those latter, of course, compose the region with which we are primarily concerned in this essay. America's withdrawal from Afghanistan is, then, certainly relevant to the UAE. And it is certainly relevant to the countries surrounding the UAE. If ever there was a time for less-developed countries to adopt locally-sourced models of success, it is now.

Another proverbial elephant in the room is, as mentioned, the Sino-American relationship. What the two great economic giants of our times decide to do with—or indeed to—each other will color all else. No aspect of international relations, or the world economy, is safe from a U.S.-China conflict. But at the same time, all can benefit if such conflict is averted. Globalization can still proceed—and proceed apace—if and only if America and China find a way to soothe their common maladies: concerns over who exactly is in charge of what despite so very many shared economic outcomes.

Globalization can still proceed—and proceed apace—if and only if America and China find a way to soothe their common maladies: concerns over who exactly is in charge of what despite so very many shared economic outcomes.

A third elephant is the degree to which an increased concentration of new patents by massive technology conglomerates consolidates power among a group of "too big to fail" and "too big to share" technology behemoths. These tech giants either become quasi-nation states of their own, willing to battle government edicts (e.g., Apple's refusal to allow the FBI to break its encryption, Amazon's tax haven fight with the European Union, or Google's tenuous approach toward the EU's data protection regulatory scheme), or they eventually become nationalized in reality or in practice when they or their charismatic owners become so big so as to pose a sovereign threat, as Alibaba and Jack Ma have learned. In fact, the urge to hoard innovation is so powerful that a cottage industry of well-financed, and often publicly listed, patent "troll" businesses have emerged. The largest of such holds hundreds of thousands of patents and has deployed advanced analytics to determine infringement globally.

So yes, global trade is not all plain sailing. And no, the horizon is not without storms. But the fundamental point remains. Even from the vantage point of the (troubled) first quarter of the twenty-first century, there are obvious cases to be made that trade is indeed a global public good. And, in furtherance of overcoming what tensions there are with cross-border economic exchange, a little bit of political will can go a very long way. We make the case for that will being present in the UAE and Israel and, too, the unashamed argument that if such will can be brought to bear, many seemingly intractable problems will be greatly reduced in the years to come.

Demonstrable Gains

As things stand today, the transfer of IP has developed something of a bad name. Largely, this is due to the increased rivalry between China and the United States. So, the argument

goes, America ought to stop sharing its ideas with the rest of the world, and especially China, lest other nations catch up or overtake its technological capacity. Implied is that other nations might also wish to follow suit. Herein, a new era of trade suspicions, if not trade wars, looms—the wider evidence for which includes events such as Brexit, the U.S.-EU trade spat over planes, trains, and automobiles, and AUKUS, the surprise announcement of a U.S.-UK-Australia nuclear submarine-sharing deal. Protectionism and conflict, of course, always walk hand in hand.

In the decades to come, everything from culture and science to entertainment and medicine will inevitably become public.

But it need not be like this. For one, America cannot stop sharing its ideas. The Jeffersonian universalism lying at the heart of its republic must, and will, evangelize. Sometimes this takes the form of exporting lofty ideas. Sometimes it takes the form of exporting cartoons. But the American project is, today, inescapably itself a presence in the world. True isolationism is dead: even as the U.S. pulls back from certain military engagements, it is doubling down on others. After all, America left Kabul only to remain in the South China Sea. Moreover, other countries cannot hide their respective IP for long, either. China, the member states of the European Union, the countries of Latin America, and so on, will continue to exist in a complicated network of trade and knowledge-sharing. In the decades to come, everything from culture and science to entertainment and medicine will inevitably become public. This will not always happen by choice; and we are moving into an increasingly fungible world of data and communications technology. In this world, most functions, assets, and even human experiences (the "metaverse") will be available in surrogate digital form. The ease by which these assets and proxies will move across sovereign boundaries will also speed up, redefining the basic notion of property rights at the individual, corporate, and nation-state levels. While any one of these trends may be stopped individually, or significantly hindered through legislative or legal action, it is unlikely that any nation-state or group of nation-states can or will be able to ban the new footprint of digital technology in the human experience.

And so, great power competition aside, there is another lens through which to look at the transfer of IP. Perhaps today this is a less popular view, but it is nevertheless the case that we have made: supporting and developing cross-border economic interactions is far from a lost cause. Quite the opposite. Rather than accepting the demise of globalization, there are demonstrable gains to be had from the transfer of IP from countries with higher GDP to those with lower.

Categorically, these gains are maximized when three conditions are met. *First*, any transfers of IP should primarily be designed to introduce or enhance civilian and humanitarian infrastructure within a climate-sustainable framework. Selling soda, whatever the market for it, is obviously far less important in the long run than ensuring the provision of safe, clean, and affordable drinking water. Market forces need not be hindered, but a hierarchy of developmental priorities can and should be imposed by public policy. This is a fundamental tenet of the concept of sustainable development.

Market forces need not be hindered, but a hierarchy of developmental priorities can and should be imposed by public policy.

Second, IP transfers should predominantly be made within discrete regions, those in which a mutually beneficial political equilibrium is absent but possible. So doing may, we speculate, even improve or encourage political cooperation, or at least reduce the obvious cause of some tensions. There is after all, in an ever-changing climate, little to lose from one last, grand stab at political cooperation.

Third, a clear methodology for, and organization of, IP transfer must be put in place. Local factors must be taken into account and—again, an unfashionable view—a planned rather than a market-based approach is necessary for the initial proliferation of relevant technologies and knowhow. This implies the need for a regional leader, one able to extend the benefits of IP without provoking on-the-ground backlash. In other words, a regional trailblazer that is able to reconcile politics and economics in the political economy of the Middle East. When it comes to regional IP transfer, the UAE is perfectly placed to take on that role in the 2020s and beyond.

The transfer of IP may not save the world. Human history will continue apace, with all its conflict and collaborations alike. But, in an era of climate change and migratory turmoil, IP transfer could save much of the Middle East. Given the region's global importance, that would be a very nice start indeed. All told, we need not be at the end of history to celebrate the liberal and open transfer of technologies and ideas. Indeed, this might only be the beginning.

Science Communication and Scientific Judgment

COVID-19 and Public Policy in Our Era of Vexed Politics

Naomi Oreskes

THE year 2020 was truly a historic one—and mostly not in a good way. Among many things, we saw a historic level of disregard of scientific advice with respect to COVID-19, which made the pandemic worse in the United States than in many other countries. But while the events of 2020 may feel unprecedented, the social pattern of rejecting scientific evidence did not suddenly appear in that year of pestilence. There was never any good scientific reason for rejecting the expert advice on COVID-19, just as there has never been any good scientific reason for doubting that humans evolved, that vaccines save lives, and that greenhouse gases are driving disruptive climate change.

Past is Prologue

To understand the social pattern of rejecting scientific findings and expert advice, we need to look beyond science to history, which tells us that many of the various forms of the rejection of expert evidence and the promotion of disinformation have roots in the history of tobacco.

Throughout the first half of the twentieth century, most Americans saw science as something that made their lives better.

Naomi Oreskes *is Professor of the History of Science and Affiliated Professor of Earth and Planetary Sciences at Harvard University. This is an expanded version of a set of essays first published in* Scientific American *magazine, including "To Understand How Science Denial Works, Look to History," "Scientists Should Admit They Bring Personal Values to Their Work," "If You Say 'Science Is Right,' You're Wrong," "Expert Opinion Can't Be Trusted if You Consult the Wrong Sort of Expert," "Making Vaccines Is Straightforward; Getting People to Take Them Isn't," and "Don't Fact-check Scientific Judgment Calls." You may follow Prof. Oreskes on Twitter @NaomiOreskes.*

At the same time, corporate America was also developing the playbook for science denial and disinformation. The chief culprit in this darker story was the tobacco industry, whose tactics have been well documented by historians of science, technology, and medicine, as well as epidemiologists and lawyers. It disparaged science by promoting the idea that the link between tobacco use and lung cancer and other diseases was uncertain or incomplete and that the attempt to regulate it was a threat to American freedom. The industry made products more addictive by increasing their nicotine content while publicly denying that nicotine was addictive. With these methods, the industry was able to delay imposing effective measures to discourage smoking long after the scientific evidence of its harms was clear. In our 2010 book, *Merchants of Doubt*, Erik M. Conway and I showed how the same arguments were used to delay action on acid rain, the ozone hole, and climate change—and starting in 2020 we saw the spurious "freedom" argument being used to disparage mask wearing.

There was never any good scientific reason for rejecting the expert advice on COVID-19, just as there has never been any good scientific reason for doubting that humans evolved, that vaccines save lives, and that greenhouse gases are driving disruptive climate change.

We also saw the tobacco strategy seeping into social media, which influences public opinion and which many people feel needs to be subject to greater scrutiny and perhaps government regulation. Without a historical perspective, we might interpret this as a novel problem created by a novel technology. But in September 2020, a former Facebook manager testified in the U.S. Congress that the company "took a page from Big Tobacco's playbook, working to make our offering addictive," saying that Facebook was determined to make people addicted to its products while publicly using the euphemism of increasing "engagement." Like the tobacco industry, social media companies sold us a toxic product while insisting that it was simply giving consumers what they wanted.

Scientific colleagues often ask me why I traded a career in science for a career in history. History, for some of them, is just "dwelling on the past." My short answer begins by citing what one of Shakespeare's characters exclaims in *The Tempest*: "What's past is prologue." If we are to confront disinformation, the rejection of scientific findings, and the negative uses of technology, we have to understand the past that has brought us to this point.

PERSONAL VALUES VS. VALUE NEUTRALITY

The notion that science is and should remain value-free has complex historical roots and has been challenged over time. Now, as the U.S. recoils from the divisions of recent years and the scientific community tries to rebuild trust in science, scientists may be tempted to reaffirm their neutrality. If people are to trust us again, as I have frequently heard colleagues argue, we have to be scrupulous about not allowing our values to intrude into our science. This presupposes that value neutrality is necessary for public trust and that it is possible. But available evidence suggests that neither presumption is correct.

Value neutrality is a tinfoil shield. Rather than trying to hide behind it, scientists should admit that they have values and be proud that these values motivate research aiming to make the world a better place for all. Francis Bacon, after all, wrote that the goal of science is the "relief of man's estate."

Recent research in communications has shown that people are most likely to accept a message when it is delivered by trusted messengers—teachers, for example, or religious or business leaders, or local doctors and nurses. One strategy to build trust, therefore, is for scientists to build links from their laboratories, institutes, and academic departments into the communities where they live and work. One way to do this—in the United States, at least—is by partnering with organizations such as the National Center for Science Education, which was founded to fight creationism in the classroom but is now working broadly with teachers to increase understanding of the nature of science itself. To do this, scientists do not need to throw off their personal values; they merely need to share with teachers a belief in the value of education. This is important because research suggests that, even if we try, we cannot throw off our values.

It is well known that people are more likely to accept evidence that accords with what they already believe. Psychologists call this "motivated reasoning," and although the term is relatively recent, the insight is not. Four hundred years ago, Francis Bacon put it this way: "Human understanding is not composed of dry light, but is subject to influence from the will and the emotions [...]. [M]an prefers to believe what he wants to be true."

Some research suggests that even with financial incentives, most people are apparently incapable of escaping their biases. Great scientists may think that because they are trained to be objective, they can avoid the pitfalls into which ordinary people fall. But that is not necessarily the case. Does this mean that science cannot be objective? No. What makes it so is not scientists patrolling their own biases but rather the mechanisms used to ensure that bias is minimized. Peer review is the best known of these, though equally if not more important is diversity. As I contend in the new edition of my book *Why Trust Science* (2021), diversity in science is crucial not just to ensure that every person has a chance to develop his or her talent but to ensure that science is as unbiased as possible.

Some will argue that value neutrality is an ideal toward which we should strive, even if we know it cannot be achieved entirely. In the practice of science, this argument may hold. But what is useful in scientific research may be counterproductive in public communication because the idea of a trusted messenger implies shared values. Studies show that U.S. scientists want (among other things) to use their knowledge to improve health, make life easier, strengthen the economy through innovation and discovery, and protect people from losses associated with disruptive climate change.

Opinion polls suggest that most Americans want many of these things, too; according to a recent reliable survey, 73 percent of those polled believe that science has a mostly positive impact on society. If scientists decline to discuss their values for fear that they conflict with the values of their audiences, they may miss the opportunity to discover significant points of overlap and agreement. If, on the other hand, scientists insist on their value neutrality, they will likely come across as inauthentic, if not dishonest. A person who truly had no values—or refused to allow values to influence their decision-making—would be a sociopath!

SCIENTIFIC METHOD AND COMMUNICATION

Value neutrality is a tinfoil shield. Rather than trying to hide behind it, scientists should admit that they have values and be proud that these values motivate research aiming to make the world a better place for all. Francis Bacon, after all, wrote that the goal of science is the "relief of man's estate."

As the COVID-19 crisis invited onslaughts against their profession, scientists have certainly found inspiration in values to defend their enterprise. But in their zeal to fight back against vaccine rejection and other forms of science denial, some scientists say things that just are not true—and you cannot build trust if the things you are saying are not trustworthy.

For instance, one popular move made by scientists is to insist that science is right—full stop—and that once we discover the truth about the

world, we are done. Anyone who denies such truths (they suggest) is stupid, ignorant, or fatuous. Well, no. Even a modest familiarity with the history of science offers many examples of matters that scientists thought they had resolved, only to discover that they needed to be reconsidered. Some familiar examples are the Earth being the center of the universe, the absolute nature of time and space, the stability of continents, and the cause of infectious diseases. Some conclusions are so well established we may feel confident that we will not be revisiting them. I cannot think of anyone I know who thinks we will be questioning the laws of thermodynamics any time soon. But physicists at the start of the twentieth century—just before the discovery of quantum mechanics and relativity—did not think they were about to rethink their field's foundations, either.

History and philosophy have shown that the idea of a singular scientific method is, well, unscientific. In fact, the methods of science have varied between disciplines and across time.

Another popular move is to say scientific findings are true because scientists use "the scientific method." But we can never actually agree on what that method is. Some will say it is empiricism: observation and description of the world. Others will say it is the experimental method: the use of experience and experiment to test hypotheses. Recently, a prominent scientist claimed the scientific method was to avoid fooling oneself into thinking something is true that is not, and vice versa.

Each of these views has its merits, but if the claim is that any one of these is the scientific method, then they all fail. History and philosophy have shown that the idea of a singular scientific method is, well, unscientific. In fact, the methods of science have varied between disciplines and across time. Many scientific practices, particularly statistical tests of significance, have been developed with the idea of avoiding wishful thinking and self-deception, but that hardly constitutes "the scientific method." Scientists have bitterly argued about which methods are the best, and, as we all know, bitter arguments rarely get resolved.

In my view, the biggest mistake scientists make is to claim that this is all somehow simple and therefore to imply that anyone who does not get it is a dunce. Science is not simple, and neither is the natural world; therein lies the challenge of science communication. What we do is both hard and, often, hard to explain. The good news is that when we fall flat, we pick ourselves up, brush ourselves off, and get back to work. Understanding the beautiful, complex world we live in, and using that knowledge to do useful things, is both its own reward and why taxpayers should be happy to fund research.

Scientific theories are not perfect replicas of reality, but we have good reason to believe that they capture significant elements of it. And experience reminds us that when we ignore reality, it sooner or later comes back to bite us.

The biggest mistake scientists make is to claim that this is all somehow simple and therefore to imply that anyone who does not get it is a dunce. Science is not simple, and neither is the natural world; therein lies the challenge of science communication.

The Political Variable

While saying "science is always right" may be incorrect, so too is repeating the familiar trope: "Experts are always getting it wrong." History shows that scientific experts mostly get things right, but examples where they have gone wrong offer the opportunity to better understand the limits of expertise. A case in point is the Global Health Security Index (GHSI), the result of a project led by the Nuclear Threat Initiative and the Johns Hopkins Center for Health Security. It was published in October 2019, just weeks before the novel coronavirus made its appearance.

GHSI researchers evaluated global pandemic preparedness in 195 countries, and the U.S. was judged to be the most prepared country in the world. The UK was rated second overall. New Zealand clocked in at number 35. Vietnam was number 50. As ensuing events showed, the experts certainly got that wrong. Vietnam and New Zealand had among the best initial responses to the COVID-19 pandemic; the UK and the U.S. were among the worst.

So what happened? The GHSI framework was based heavily on "expert elicitation"—the querying of experts to elicit their views. (This method contrasts with consensus reports, which are primarily based on a review of existing, peer-reviewed publications.) Expert elicitation is often used to predict risks or otherwise evaluate things that are hard to measure. Many consider it to be a valid scientific methodology, particularly to establish the range of uncertainty around a complex issue or—where published science is insufficient—to answer a time-sensitive question. But it relies on a key presumption: that we have got the right experts.

The GHSI panel was understandably staffed heavily with directors of national and international health programs, health departments, and health

commissions. But the experts included no professional political scientist, psychologist, geographer, or historian; there was little expertise on the political and cultural dimensions of the problem. In hindsight, it is clear that in many countries, political and cultural factors turned out to be determinative.

The United States—a country with some of the most advanced scientific infrastructure in the world and a prodigious manufacturing and telecommunications capacity—failed to mobilize this capacity for reasons that were largely political. Initially, then-President Donald Trump did not take the pandemic seriously enough to organize a forceful federal response, and then, by his own admission, downplayed it. America's layered and decentralized system of government led to varied policies, in some cases putting state governments in conflict with their own cities. And many refused to practice social distancing, interpreting it as an infringement on their freedom.

To evaluate American preparedness accurately, the GHSI group needed input from anthropologists, psychologists, and historians who understood American politics and culture. Around the globe, whether countries were able to mount an effective pandemic response depended crucially on governance and the response of their citizens to that governance. The GHSI team got it wrong because the wrong experts were chosen.

The Perplexity of Human Behavior

Just as the experts on the GHSI team failed to consider the relevant and ultimately decisive human element in the COVID-19 battle, the uptake of vaccines proved to be more complicated than simply making the technology available. Vaccine uptake, and especially the widespread acceptance of vaccines, is a social endeavor that requires consideration of human factors.

Vaccine uptake, and especially the widespread acceptance of vaccines, is a social endeavor that requires consideration of human factors.

However, questions involving human behavior are some of science's most perplexing. There is a saying in the field of artificial intelligence: "Hard things are easy; easy things are hard." Activities that most people find very hard, such as playing chess or doing higher mathematics, have yielded fairly readily to computation, yet many tasks that humans find easy or even trivial resist being conquered by machines.

Twenty-five years ago, Garry Kasparov famously became the first world chess champion to lose to a computer. Today, computer programs can beat the world's best players at poker and Go, write music and even pass the famous Turing test—fooling people into thinking they are talking to another human. Yet computers still struggle to do things most of us find easy, such as learning to speak our native tongue or predicting from body language whether a pedestrian is about to cross the street—something that human drivers do subconsciously. Still, that can stymie even the most advanced self-driving cars.

AI researchers will tell you that chess turned out to be comparatively easy because it follows a set of rigid rules that create a finite (albeit large) number of possible plays. Predicting the intentions of a pedestrian, however, is a more complex and fluid task that is hard to reduce to rules. No doubt that is true, but I think there is a bigger lesson in the AI experience that applies to more urgent problems. Let's call it the vaccine-vaccination paradox.

Anyone familiar with biology is hugely impressed by the agile scientific work that in under a year yielded astonishingly effective vaccines to fight COVID-19. Both the Moderna and the Pfizer-BioNTech vaccines use messenger RNA (mRNA) to deliver instructions to cells to generate the spike protein found on the novel coronavirus, which prompts the body to make the antibodies needed to fight an actual infection. It is a brilliant piece of biotechnological work that bodes well for similar uses of mRNA in the future.

Yet, even now, after more than a year after those vaccines were cleared for use, it is extremely hard to get the American population fully vaccinated, much less boosted. In the United States, the difficulties have included the vexed politics of the past several years, but the logistical challenges turned out to be great as well. Before the vaccines were authorized, some health experts were concerned that there might not be enough vials and syringes or cold storage. Others noted the problem of vaccine hesitancy. And since the vaccines became available, a host of new problems, including such quotidian tasks as scheduling, have plagued the program. The hard task of creating a vaccine proved (relatively) easy; the easy task of vaccination has proved very hard.

In light of the above, maybe it is time to rethink our categories. We view chess as hard because very few people can play it at a high level, and almost no one is a grand master. In contrast, nearly all of us could probably learn to drive a truck to deliver vaccines. But this perspective confuses difficulty with scarcity. As the AI example shows, many things that all of us can do are in some respects remarkably difficult. Or perhaps we are conflating what is difficult to conceive with what is a challenge to do. Quantum physics is conceptually

hard; administering 600 million shots in a large, diverse country with a decentralized health system is a staggeringly difficult practicality.

We call the physical sciences "hard" because they deal with issues that are mostly independent of the vagaries of human nature; they offer laws that (at least in the right circumstances) yield exact answers. But physics and chemistry will never tell us how to design an effective vaccination program or solve the problem of the crossing pedestrian, in part because they do not help us comprehend human behavior. The social sciences rarely yield exact answers. But that does not make them easy.

When it comes to solving real-life problems, it is the supposedly straightforward ones that seem to be tripping us up. The vaccine-vaccination paradox suggests that the truly hard sciences are those that involve human behavior.

Don't Fact-check Scientific Judgment

While the salient issue of our unprecedented times is convincing people of the right facts to get shots in arms, sometimes the struggle is simply deciding on what the facts are. In a world that has become relentlessly "truthy," to borrow Stephen Colbert's apt neologism, we need journalists, scientists, and other experts to stand up for facts and keep the public debate honest. But this has proved to be a daunting task, especially with regards to issues such as climate change, where there is a tricky gray zone between facts and expert judgments.

One such zone has been on display since the release of a 2018 Intergovernmental Panel on Climate Change (IPCC) special report entitled Global Warming of 1.5 °C, whose authors concluded that we had 12 years left (now 8) to achieve radical reductions in greenhouse gas emissions to limit global warming. This alert has been widely cited, and politicians who have invoked it have been repeatedly fact-checked. But some of this checking made the dialogue feel more like ice hockey—where the "checking" was intended to disrupt play and establish dominance—than like an effort to help the public understand a complex but crucial issue.

In the 2020 presidential election's second Democratic debate, for example, former U.S. Representative Beto O'Rourke of Texas said, "I listen to scientists on this, and they are very clear. We don't have more than 10 years to get this right." And Pete Buttigieg, at the time the mayor of South Bend, Indiana, said, "Science tells us we have 12 years before we reach the horizon of catastrophe when it comes to our climate." The *New York Times* declared that both statements were "misleading," insisting that any claim "that there are 12 or just 10 years until the point of no return goes beyond what the [IPCC] report itself says." The *Washington Post* called 12 years "a figure that is frequently cited but often misused," implying that Buttigieg was among those referencing it in error.

But the IPCC was not stating a fact in the first place. It was presenting a collective expert judgment—in this case, the consensus of 86 authors and review editors from 39 countries. Given this accounting, there will inevitably be a range of legitimate interpretations. With the finding understood in this way, the dynamic of fact-checking is misplaced. It would be as if after 9/11, the media were fact-checking how politicians characterized the threat to America.

The vaccine-vaccination paradox suggests that the truly hard sciences are those that involve human behavior.

Moreover, consider the headlines that news outlets themselves offered when the report came out. From the *New York Times*: "Major climate report describes a strong risk of crisis as early as 2040." The AP: "UN report on global warming carries life-or-death warning." And just for fun, here is what the *New York Post* had to say: "Terrifying climate change warning: 12 years until we're doomed."

Call me unfussy, but these headlines do not strike me as substantively different from what the politicians said. They use the same language of crisis, of time limits, and of life and death that the fact-checkers rejected. And contrary to the AP report, scientists did, in fact, agree on a time frame.

Politicians do sometimes say things that are egregiously at odds with expert consensus; the overt denial of climate change is the obvious case in point. We should call out conspicuously false claims, such as an assertion that the world will end tomorrow (it might, but not from climate change), but let's not fact-check things that are not facts. There is a world of interpretation—and therefore a range of justifiable readings—built into any expert judgment. We should discuss that reasonable range and flag claims that are obviously unreasonable. But we should not confuse judgments with facts. Doing so turns what should be a serious discussion into a score-driven hockey brawl.

The same argument, of course, can be made with regards to the vaccine issue and pretty much every other aspect of the fight against COVID-19. And that's the overall point of this essay. But at the end of the day, discounting much less disregarding expert judgment on a pandemic or any other issue that requires scientific as well as public policy input will do much, much more harm than good. What is my evidence? Well, again let me quote from *The Tempest*: "What's past is prologue."

HORIZONS

Editorial Internship Program

The publisher of *Horizons*—the Center for International Relations and Sustainable Development (CIRSD)—is seeking top-caliber individuals to serve as editorial interns in our main office, located in Belgrade, Serbia.

Editorial interns are fully integrated into the editorial work of *Horizons*, providing a unique opportunity for highly-motivated individuals to gain valuable, real-world work experience in a diverse and results-oriented environment.

Editorial interns will gain experience in all aspects of the publication process—from editing to research and production.

Responsibilities typically include:

- researching potential articles and authors;
- reviewing and copyediting articles;
- fact-checking submissions;
- maintaining media and other databases;
- supporting webmaster and helping with social media promotion;
- assisting with issue layout;
- writing blog posts.

Applicants should possess the following qualifications:

- demonstrated serious interest in international affairs and foreign policy publications;
- exceptional English-language writing and editing skills;
- strong organizational and research skills;
- ability to multitask within deadlines and work well with others;
- autonomous, proactive, intellectually curious, and responsible;
- matriculation in an academically-rigorous college or university (both undergraduate and graduate students may apply).

Prospective applicants should contact
Horizons Editor Damjan Krnjević Mišković
at damjan.krnjevic@cirsd.org for general queries,
additional information, and to submit their applications.

Please include a résume and cover letter.

cirsd.org

Start and ending dates for *Horizons* editorial interns are flexible.
Availability should be indicated in the cover letter.

cirsd
CENTER FOR INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

The CIRSD Internship Experience

One of the most prestigious programs of its kind in Southeast Europe

CIRSD has one of the most prestigious and intensive internship programs in Southeast Europe. We are fortunate to continue to attract a talented, eloquent, multilingual, and diverse group of exceptional young women and men who have been educated at top universities from around the world.

Our interns are or have studied at world-renowned universities like Harvard University, Oxford University, Columbia University, Georgetown University, Zhejiang University, Tsinghua University, Duke University, Sciences Po, and the University of Vienna, as well as Duke Kunshan University, Trinity College (Hartford), the Georgia Institute of Technology, the University of Bristol, the University of Belgrade, and the University of Sarajevo.

Our internship program offers a plethora of exciting opportunities for students, recent graduates, and young professionals to broaden their public policy and research skills—crucial to advancing career prospects in diplomacy, international relations, and sustainable development.

CIRSD is a place where young, inquisitive minds can sharpen their leadership and communication skills while gaining practical, hands-on experience with the help of committed mentors and seasoned professionals.

For general queries, additional information, and to submit an application, please send an email to:

Ms. Anja Jević, CIRSD Associate Director & Director of the CIRSD Internship Program:
anja.jevic@cirsd.org

A Personal Reflection on Afghanistan

Richard Haass

A LITTLE over five years ago, I authored *A World in Disarray*, whose Serbian language edition was subsequently published by the Center for International Relations and Sustainable Development (CIRSD). The book's thesis was that the Cold War's end did not usher in an era of greater stability, security, and peace, as many expected. Instead, what emerged was a world in which conflict was much more prevalent than cooperation.

Some criticized the book at the time as being unduly negative and pessimistic. In retrospect, it could have been criticized for its relative optimism. The world today is a messier place than it was five years ago—and most trends are heading in the wrong direction. One of these is Afghanistan, which appears to be on its way to becoming again a world leader in terrorism, opium production, and misery.

The Biden Administration's poorly executed withdrawal from Afghanistan resulted in a lively debate on a whole host of issues related to the conduct of American foreign policy. Some have even questioned whether the United States was right to go into Afghanistan in the first place. For me, the answer was and remains unambiguous: we were 100 percent right to go in. The Taliban, which ruled Afghanistan at the time, harbored terrorists who attacked the United States and killed nearly 3,000 civilians. That attack had to go answered. Also important was the precedent the United States established, namely that it would not distinguish between terrorists and those who supported them. The United States gave the Taliban a choice—they could hand over the terrorists responsible and be spared—but they chose wrongly: a fateful decision for them.

Richard Haass *is President of the Council on Foreign Relations. He previously served as Director of Policy Planning for the U.S. State Department and was U.S. President George W. Bush's Coordinator for the Future of Afghanistan.* *This essay is based on the "Why it Matters" podcast, episode "Perspective on Afghanistan, with Richard Haass."* *You may follow Dr. Haass on Twitter @RichardHaass.*

Photo: CIRSD

CIRSD President Vuk Jeremić and CFR President Richard Haass in Belgrade in January 2018

Moreover, we made the right decision to help the Afghans forge their own government; if we did too much, our effort would have lacked legitimacy. That was the only clear thing, though. We did not think through what we would do afterwards. There was no clear plan and no consensus within the Bush Administration over the trajectory of U.S. policy. How ambitious should we be? What was our definition of success at that point? That is where things began to break down. That being said, however, I emphasize that the War on Terror, which became an important part of American foreign policy, did result in America becoming effective at diminishing the threat posed by terrorism to the United States.

The War on Terror quickly took on a global dimension—with a focus in parts of the Middle East and Africa—because that is where various terrorist cells had set up shop. We discovered that groups like al-Qaeda and others were international. They had access to money, guns, and people.

That phase of American foreign policy began over twenty years ago, and it is still ongoing—largely but not exclusively in the Middle East and Africa, but also in parts of Asia. To my mind, the

struggle against terrorism is open-ended. There are some parallels with our current battle against COVID-19. You don't eliminate terrorism any more than you eliminate a virus. These are now baked into the world of the twenty-first century.

Terrorism, in other words, is a global and open-ended challenge, although it had been centered in Afghanistan for a moment during which it had come to us most painfully and vividly. Afghanistan was where the terrorists involved in 9/11 had been trained. They were not Afghans, however: most were from Saudi Arabia and elsewhere in the Middle East. But they were supported and organized in Afghanistan, and their leader, Osama bin Laden, was in Afghanistan. Yet after the flight of the Taliban and al-Qaeda from that country—most of them quickly escaped to neighboring Pakistan—Afghanistan was no longer the epicenter of world terrorism. Terrorism had essentially dispersed.

The Taliban harbored terrorists who attacked the United States and killed nearly 3,000 civilians. That attack had to go answered. Also important was the precedent the United States established, namely that it would not distinguish between terrorists and those who supported them. The United States gave the Taliban a choice—they could hand over the terrorists responsible and be spared—but they chose wrongly.

Thus, over time, America's reasons for being in Afghanistan changed. Competing views emerged on what should be done after the initial phase had ended. In many ways, what was done, or not done, has come back to haunt us in many ways.

Let me recapitulate. America and its allies had successfully worked with our Afghan partners, removed the old authority (the Taliban), and helped bring about a new authority led by Hamid Karzai. And then the question became: what do we do next? Not just in the context of Afghanistan but in the context of the Taliban. The feeling was that the United States could not just leave the Taliban be, because we knew that they had crossed into Pakistan. And the question was also, how do we help the new authorities in Afghanistan stand up? In other words, how do we build them up so that Afghanistan could become something approximating a normal country?

We were not talking about democracy at this point; we were talking about building up the capacity of this first post-Taliban government, so that it could police its borders and its national territory, so that terrorists would not be able once again to use Afghanistan as a piece of real estate.

I painfully and vividly remember the debates we had within the Bush Administration on these questions—on, to put it bluntly, the question of how ambitious America should be in its approach to Afghanistan. One of the common phrases used, then and now, is "nation-building" or "state-building," but, in reality, that was capacity-building. The question was formulated in the following manner, more or less: What kind of capacities ought we try to bring about in Afghanistan?

I painfully and vividly remember the debates we had within the Bush Administration on these questions—on, to put it bluntly, the question of how ambitious America should be in its approach to Afghanistan.

What I proposed was that the United States and its allies would stay in Afghanistan temporarily and perform two functions. The *first* was that we would help the new government consolidate authority over Afghan real estate, because it is a large country—it is, for instance, more than twice the size of Poland, but its terrain is much more prohibitively mountainous. The *second* function was that we would help develop and train the Afghanistan armed forces. At that point, it was not clear how national its military would be, as opposed to regional, but the point was that America would help stand up an Afghan army.

Without getting into the details, suffice it to say there was remarkably little enthusiasm for doing what I had proposed. Now, admittedly, I was used to being unsuccessful in my policy proposals, but even in my career of unsuccessful attempts to influence U.S. foreign policy, this stood out. It was one of the most painful national security meetings I had ever attended. There just was not any enthusiasm.

If I had to boil down the takeaways from the discussions that took place during that period, I would say that this lack of enthusiasm reflected two things. The *first* was pretty legitimate and can be formulated as a question: why do we want to get ambitious in Afghanistan? The counter-argument went along these lines: this is a country with little tradition of a strong central government. Afghanistan is very tribal and regional, and it is, simply put, the wrong place for us to get ambitious. And, in retrospect, I think that was a legitimate concern. The *second* concern that was raised in response to my proposal—a concern that was less legitimate, in my view—was that there was much more excitement about getting involved more in other parts of the world, i.e., Iraq. And the feeling was that Iraq was a place where if America

did invest sufficient resources, then the United States would have more to show for it. In other words, Iraq was a potential democracy—it was a potential model that other Arab countries might emulate. In contrast, Afghanistan was seen as an isolated one-off.

The bottom line was that Afghanistan was seen as both a poor prospect and a poor investment.

Another part of the argument I made was that we had a window: the Taliban had been routed and the new governing authority's legitimacy was really high. We needed to build up authority. My point was that America could not remove a government and then not put something in its place.

For those who question that argument, I have a one-word response: Libya. Under the Obama Administration, the United States went in and removed Muammar Gaddafi and never put anything in his place. As a result, Libya became—and remains—a failed state. And what we learned in some cases is that bad situations can get worse. Thus, my view on Afghanistan—I did not have the Libya example at the time—was that we had to try to do something that was neither overly ambitious nor under-ambitious. My point at the time was that the United States had a moment, and that we needed to harness it. I thought that we would have had significant international help, and I felt that what I was proposing we do could be accomplished in relatively short order. But again, there was simply no enthusiasm for it.

America's reasons for being in Afghanistan changed. Competing views emerged on what should be done after the initial phase had ended. In many ways, what was done, or not done, has come back to haunt us in many ways.

What ended up happening subsequently was that the rate of nation- or capacity- or army-building in Afghanistan was incredibly slow. Meanwhile, this was not happening in isolation: with sanctuary across the border in Pakistan, the Taliban was rebuilding and reconstituting at a pretty good clip.

Pakistan had gone back to business-as-usual regarding the Taliban: it was operating openly out of Pakistani cities—what was then known as the North-West Frontier Province of Pakistan became one giant sanctuary for the Taliban. (For a while after 9/11, Pakistan had cleaned up its act regarding the Taliban, in part because senior members of its government happened to have been in Washington on 9/11, and, as one can imagine, very frank conversations were held with them at the time by the likes of Deputy Secretary of State Richard Armitage.)

The historical record is clear: it is very hard to prevail in a "civil war" if one of the parties has access to a cross-border sanctuary. This is in fact what the Taliban were able to accomplish.

The point is that we had two parallel dynamics: on the one hand, a very slow one of building up government capacity, and, on the other hand, a fast and unhealthy one of the Taliban reconstituting itself, in part because the U.S. military had failed to stop them from escaping. Then we took our eye off the ball and Pakistan went ahead and allowed the Taliban to regroup and rebuild.

Americans tend to see situations as problems, and anytime we hear the word "problem," we immediately expect to see the word "solution." And the problem with thinking of things as problems, as it were, is that lots of things are really situations, and, by definition, situations cannot be solved with military force or any other policies. At best, situations can be managed.

This was more or less the state of play at the time I left my post as U.S. Coordinator for the Future of Afghanistan and Director of Policy Planning at the State Department in June 2003. By the time the Obama Administration came to power, the Taliban had resumed all sorts of efforts within Afghanistan. The situation was beginning to deteriorate, and by then America had made the fateful decision to dramatically increase U.S. forces—a policy initiative that became known as the "surge." There were three basic problems with this policy, which was announced in late 2009 and became operational in early 2010: *one*, by then America had clearly overstayed its welcome in Afghanistan; *two*, we had allowed the Taliban to rebuild; and *three*, the fact that we were surging forces increasingly involved in combat against a reconstituted Taliban meant that U.S. casualties increased and the cost of the war by every definition of the word "cost" went way up. Thus, Afghanistan went from being the "good war" to being simply the second bad war (with the first being the Iraq War).

In testimony that I gave to the U.S. Senate Foreign Relations Committee in May 2011, I argued that, at this point, the United States should aim for an Afghanistan that was "good enough," given local realities, limited American interests, and the broad range of both domestic and global challenges facing the United States.

My argument was based in part on an assessment that the surge amounted to an attempt to be decisive in a situation in which I did not think America could be decisive—that the surge was not going to end in a military victory in which

the Taliban would sue for peace. In this period, I was instead arguing for something more modest—something "good enough" for both Afghanistan and Iraq.

Americans tend to see situations as problems, and anytime we hear the word "problem," we immediately expect to see the word "solution." And the problem with thinking of things as problems, as it were, is that lots of things are really situations, and, by definition, situations cannot be solved with military force or any other policies. At best, situations can be managed. This often means not what you can bring about, but what it is you can avoid. The phrase "good enough" was meant to convey that idea—that the United States needed to dial down its ambitions and simply say: what we want to avoid is a Taliban takeover of the major cities; we cannot stop the Taliban from making some inroads; but we can establish a situation that we can help sustain at an affordable cost. That is why I argued against the surge policy.

My capacity-building proposal, made in the wake of 9/11, was by no means guaranteed to work; but I thought it was worth a limited investment. I did not think it was a high-risk endeavor at that moment because the United States had tremendous authority and momentum and because both the Taliban and al-Qaeda were gone.

The idea animating its proponents, in contrast, was that a decisive blow was possible. And the reality was that it was not. Part of my thinking was informed by an insight made by Colin Powell—he was Secretary of State when I worked at the State Department and, prior to that had been Chairman of the Joint Chief of Staff—to the effect that military force is good at destroying things and in turn at creating a favorable context in which other things can happen. My own view derives from this insight, namely that the United States turns to its military too often.

This is not to imply that nation-building cannot work; but it works only in the right circumstances: its most famous successes were in defeated, occupied countries like Germany and Japan after World War II. Asking why it worked there, one might examine the characteristics of those societies: they were highly educated and highly homogenous; and they were both societies with strong national traditions, and so forth.

I perfectly understand that none of these things were present in Afghanistan in 2001. My capacity-building proposal, made in the wake of 9/11, was by no means guaranteed to work; but I thought it was worth a limited investment. I did not think it was a high-risk endeavor at that moment because the United States had tremendous authority and momentum and because both the Taliban and al-Qaeda were gone. As I have already said: I thought there was a window, and my view was, "let's take advantage of this window. Worse comes to worst, it won't work, which will still leave us in an advantageous position to deal with the consequences."

Our unwillingness to give it a serious try set in motion a situation in which Afghanistan's new government was never able to do what it needed. We misguidedly took on an ever-larger role in Afghanistan, which meant that we became not only behind-the-scenes nation-builders but also essentially a protagonist in the country's civil war. And that seemed to me an escalation that was unwise.

All wars are fought three times. There is the political struggle over whether to go to war. There is the physical war itself. And then there is the struggle over differing interpretations of what was accomplished and the lessons of it all.

In 2010, I wrote a book called *War of Necessity, War of Choice* in which I argued that all wars are fought three times. There is the political struggle over whether to go to war. There is the physical war itself. And then there is the struggle over differing interpretations of what was accomplished and the lessons of it all. In reflecting on the U.S. withdrawal from Afghanistan, what worries me is that we could end up learning the wrong lessons.

I do not believe the lesson ought to be that nation- or state-building is always wrong—that it's always destined to fail. I think what we really need to think hard about on the basis of Afghanistan can be formulated as a set of questions. What are the conditions that we think are positive? What are the techniques? What have we learned about sequencing? What have we learned about pacing? What have we learned about how to adjust for local culture and history?

The reason this is so important, in my view, is that we do not want to be doing everything ourselves around the world. At the same time, there are dozens of governments around the world we need to help—particularly in the Middle East, Central America, and Africa. And so, we had better learn some of the correct lessons of nation-building rather than to conclude either that it is never worth it or that it is never a good idea.

It seems to me that there are only two alternatives to learning the right lessons from Afghanistan: either we accept that we will live in a world that is much more dangerous, or we confront ourselves with having the United States get involved directly in combat operations in more places.

Such reflections touch upon one of the fundamental debates in American foreign policy. Again, we can formulate this as a set of questions: What responsibilities do we have to a society and to a culture when we come into a country and leave? To what extent should American foreign policy be about shaping and influencing the external behavior of other countries? And to what extent should what we do in the world be about influencing the domestic behavior of other states?

The way to answer any of these questions lies first in understanding that American influence is often limited and that the United States often has other priorities.

The next step involves acknowledging that perhaps the single-most ambitious task that America can imagine setting for itself is to try to change the internal workings of another society—particularly one with a long and deep culture. This does not mean U.S. foreign policy should dismiss the importance of American values, but it does mean that America must understand that there are limits of our influence—that we cannot always translate our preferences.

I'm not saying I like where this line of reasoning takes me, but that does not make it incorrect.

I still remember a dinner party that took place some time ago at which I made some version of the above argument about the Middle East. I think it would be fair to say that I was excoriated and hammered by a prominent former policymaker who was also present. His argument was, basically, that I was selling short the people in the Middle East. And I was actually accused of a kind of racism for my argument that, in effect, not everybody was ready for democracy now. My response was that I was not making a statement about individuals but rather about cultures and societies.

In some sense, of course, I do like the notion that a transformation can come about, or at least be triggered, simply by reading a translation of the Federalist Papers. *But I am not willing to believe this will necessarily happen.*

In some sense, of course, I do like the notion that a transformation can come about, or at least be triggered, simply by reading a translation of the *Federalist Papers*. But I am not willing to believe this will necessarily happen. And that is why I believe the United States has to decide what are the limits to our influence; we have to define our priorities; and we have to ask questions like, what are those things that American foreign policy is well suited to do, and what are those things that are within reach?

The withdrawal from Afghanistan and the abandonment of many Afghans most vulnerable to Taliban reprisals (e.g., women and girls, first and foremost, but really Afghans of any gender who wanted to have a twenty-first century life) worries me and causes me to wonder about American limits more broadly—not just in the context of Afghanistan.

We need to think about the fact that, for instance, we cannot convince a country like Myanmar to change its ways, notwithstanding the discrepancy between the power of the United States and the power of Myanmar. We cannot oust the military junta that took over there. The lesson here is quite basic: there is a limit to American influence in the world. The United States may very well be on the side of right and morals and virtue, but that is not necessarily the way history plays out.

There are obviously things that America can do: military intervention aside, tools of influence (both carrots and sticks) include sanctions, foreign aid, and educational opportunities. But the point is that there are still limits.

In the contemporary Afghanistan context, we know the Taliban are reimposing Sharia Law and are forcing women to wear a niqab. And we might respond to such policies by imposing one or another penalty or withhold this or that form of assistance or aid. Yet there is little to prevent them from turning to other states for the type of external support they need—states like Pakistan, Russia, or China that tend not to care about such things and have other priorities.

This means that the United States can have an Afghanistan policy in part that tries more directly to promote certain behaviors, certain norms, and certain standards; but this should not come at the price of sacrificing America's most important priority in Afghanistan: to ensure the country does not again become a place from which terrorist can operate. This has to remain the single most important thing.

That is a more classic foreign policy interest. And as we showed after 9/11, the United States has the mechanisms to act if the Taliban chooses again to harbor terrorists. The Taliban may or may not have internalized that lesson. But no one is going to launch an intervention in Afghanistan over the reimposition of Sharia Law or the fact that women are again being treated abominably—as tragic as that is.

This is where we are now—the point to which we have come, at least in the context of Afghanistan. It is

not what I would have preferred. That is one of the reasons why I had favored the United States maintaining a small presence in Afghanistan—not because it would have meant peace or because it would have led to a military victory, but because I thought that it would avoid some of the scenes that we have been seeing since the summer of 2021. And that, to me, was a consideration in my argument for maintaining a small presence—the fate that would likely befall girls and women, as well as men in Afghanistan.

The agreement negotiated by the Trump Administration to get America out and undercut the Afghan government asked virtually nothing of the Taliban. What the Trump Administration negotiated and signed was not a peace agreement; it was an American withdrawal agreement.

Obviously, this was a point on which I differed with the Biden Administration's policy on Afghanistan. Its argument was, basically, that the United States is no longer prepared to have American forces stay in Afghanistan any longer—and potentially putting themselves in harm's way—in order to deal with non-terrorism issues, as gut-wrenching as they are. That it was one thing to deal with Afghanistan as a terrorist haven and something else to deal with it as a human rights nightmare. With regards to the latter, President Biden basically said, 'we will turn to diplomacy.' Well, quite honestly, diplomacy is not going to accomplish much.

To be fair, President Biden inherited a kind of 'you can't have your cake and eat it, too' situation. We had a small military presence. Americans hadn't been doing combat operations for several years prior to his election. We had not had a combat fatality for one and half years, at that point. And we had managed to get to a point where the benefits and the costs were not out of alignment, and one of the benefits was that the quality of life for Afghan girls and women was improving.

President Biden was not willing to take the risk that the costs of a continued small American military presence would go up. He obviously did not want to face the decision of having to increase U.S. forces if the security situation deteriorated, so he essentially initiated a policy that, in my view, brought about a set of truly terrible outcomes. And my guess is he would say, 'I don't like these outcomes any more than you do, but I just wasn't willing to take the risk of what the price would be of our staying.'

It would be wrong to say these are not a legitimate set of concerns or that there was no legitimate debate that could have been had about the merits of the agreement signed by the Trump Administration in February 2020—but not over the way the withdrawal was designed and implemented, which was terrible. The agreement negotiated by the Trump Administration to get America out and undercut the Afghan government asked virtually nothing of the Taliban. I was the U.S. envoy to the Northern Ireland peace talks: we asked much more of the provisional IRA in Northern Ireland than we ever asked of the Taliban: we demanded a cease fire and we demanded that they give up their arms. We did neither with the Taliban.

I wish Americans were more consistently interested in the world, particularly since the world is interested in us—for good and bad. The latter seems to me simply to be a fact of life.

What the Trump Administration negotiated and signed was not a peace agreement; it was an American withdrawal agreement. I thought the Trump Administration was dead wrong to do it. I thought President Biden, who has had no trouble distancing himself from other things he inherited from President Trump on issues like Iran, climate change, the World Health Organization, and so on, should have distanced himself from this. Instead, he essentially, followed through on what President Trump had wrought.

One argument that those who defended the withdrawal made was that public opinion surveys indicated many Americans were in favor of getting out of Afghanistan. But this was not an intense sentiment—a driving concern—that, for instance, affected the way people voted in the presidential election. In fact, I think that if pollsters asked Americans whether they wanted their country to get out of most places, the answer would be similar. But again, the issue of intensity comes up: for example, the protests that took place in America in 2020 and 2021 had to do with race and policing issues. They were not about Afghanistan. No one in America was protesting the war in Afghanistan like Americans had protested the Vietnam War.

The question of public approval of the Biden Administration's withdrawal plans also touches upon another aspect of U.S. policymaking: traditionally, neither foreign nor domestic policy is conducted on the basis of short-term popularity. After all, we do not have referenda every day in America, or anywhere else, for that matter. In the United States, we have a representative government, and our leaders are given the responsibility to make tough decisions. The fact that Americans may today say they like that we're out of Afghanistan does not mean they will like it in a couple of years if we

face problems of terrorism at home, or if human rights atrocities happen in Afghanistan.

That being said, I wish Americans were more consistently interested in the world, particularly since the world is interested in us—for good and bad. The latter seems to me simply to be a fact of life. And the reason foreign policy is so important for America is that what we do and do not do has an impact on the world. There's a loop there: the world influences us, and we can influence the world.

It is important to come away from Afghanistan with the right lessons for American foreign policy. The only thing worse than making mistakes is not learning from them.

And I think what's interesting about Afghanistan, if we look at the last 20 years, is that there have been some moments when we got it right—e.g., initially after 9/11. But I also think that along the way we have both done too little and too much—we have over-reached and we have under-reached.

And since around the start of 2020, the United States has done a lot of under-reaching. And I think early on—so, say, between 2001 and 2003—we also under-reached in aspects of the nation-building project (I know this is a controversial view, but I think it's quite a defensible one). And clearly, with the surge and other things, we overreached: we put too many forces into the country at an inopportune moment.

My bottom line is that it is important to come away from Afghanistan with the right lessons for American foreign policy. The only thing worse than making mistakes is not learning from them.

FLAGSHIP CIRSD ARMCHAIR DISCUSSION

"Regulating Blockchain: Beyond the Politics of Crypto"

WITH
FOUNDER & CEO OF BINANCE
CHANGPENG CZ ZHAO
&
CIRSD PRESIDENT
VUK JEREMIĆ

On 20 November 2021, CIRSD was exceptionally proud to host its flagship Armchair Discussion featuring Changpeng CZ Zhao, *Founder and CEO of Binance, the world's largest cryptocurrency exchange.*

This incredible, path-breaking discussion was part of Global Town Hall 2021 (GTH2021.com), a full day international discussion of current affairs in which the world's top political, business, and intellectual leaders had a unique opportunity to connect with an audience of millions from across the globe.

IRREMEDIABLY SHAKEN?

INTERVENTION IN THE POST-AFGHANISTAN ERA

Jean-Marie Guéhenno

THE lamentable end of Western engagement in Afghanistan is a watershed event that may well mark the end of an era. At the moment, there is a lazy consensus that "intervention" in the lives of others can only fail. The same question keeps being asked: why engage in costly open-ended engagements when we don't know what we're doing? Such a mindset fits very well with the spirit of our times, a shrinking and often xenophobic vision of a world of which we are fearful because we do not understand it and are incapable of managing it: we would rather hunker down behind tightly-controlled borders than venture into dangerous foreign lands.

This is the exact opposite of the zeitgeist that prevailed in the immediate aftermath of the end of the Cold War when the triumphalist mood of the time generated a sort of hubris in the West. We thought that we could reshape the world in our own image, according to a sequence in which military intervention was followed by stabilization and came to a conclusion with the conduct of free and fair elections that would legitimize an inclusive government. We believed, in short, in social engineering.

As the head of UN peacekeeping during its biggest expansion (2000-2008), I played my part in that project, deploying multidimensional missions in a number of countries in various parts of the developing world. And if some unsavory ruler challenged that post-Cold War ambition, so the thinking went, he would need to be crushed and, if possible, tried in an international court. The emerging doctrine of the Responsibility to Protect and the creation of the International

Jean-Marie Guéhenno *is Arnold A. Saltzman Professor of Practice in International and Public Affairs at the School of International and Public Affairs (SIPA) at Columbia University and Director of SIPA's Kent Global Leadership Program on Conflict Resolution. He is a former French diplomat who served as UN Under-Secretary-General for Peacekeeping Operations and President and CEO of the International Crisis Group. You may follow him on Twitter @Jguehenno.*

Photo: Guliver Image/Getty Images

British, Turkish, and American soldiers assist an Afghan child at the Kabul airport, 20 August 2021

Criminal Court were two illustrations of that vision: the establishment of a genuine "international community" that would coalesce around shared principles and would be strong enough to show solidarity when populations were under threat.

Of course, the reality never fully conformed to that ideal model. But there was a sense that the world was shrinking and that interdependence made abstention impossible. For some, international engagement was a moral imperative whilst for others it was a strategic necessity. Either way, shoring up "fragile states"—as they were patronizingly described in advanced democracies—was not only the moral thing to do; it was also prudent because these "fragile states" might otherwise become safe-havens for transnational terrorist organizations, as had been the case when the Taliban hosted Al Qaeda and Osama bin Laden. And that might require a military intervention.

That sort of interventionism had old roots that preceded the East-West confrontation structuring the world after World War II, and of which the Soviet Union was an alternate incarnation rather than its opposite. It reflected the European tradition of universalism:

a belief in universal values that finds its secular expression in political systems. It was almost a moral obligation to spread the values that underpin them. Strategy and morality had since the early days of colonialism been blended in a morality tale, the "white man's burden" celebrated by Rudyard Kipling: the Afghan woman that appeared on the cover of Time magazine at the end of 2002 was only the last incarnation of that story, when she became the standard bearer of Western interventionism.

Because we oversold the vision of an international community, we are slightly embarrassed by our betrayal, and try to find excuses to it.

The abrupt departure from Kabul, with desperate Afghans clinging to departing airplanes and falling to their death when the planes took off, provides a brutal and gruesome ending to that morality tale. In the end, we care more about our own fellow citizens than we care about people we have never met, living in countries we can barely identify on a map. Because we oversold the vision of an international community, we are slightly embarrassed by our betrayal, and try to find excuses to it. U.S. President Joe Biden thus explained that it was difficult for America to fight for Afghanistan when Afghan soldiers were not willing to fight for their own country. He did not mention that Afghan security forces had suffered more than 70,000 casualties over the past 20 years whereas American ones had been less than 2,500. But the United States and the West felt better convincing themselves that the people they were abandoning no longer deserved their sympathy.

The truth is that the comfortable view that ethics and strategic interests converge has been blown to pieces. The horizon of reason is not the horizon of our emotions, nor is it the horizon of our interests. What we celebrate as universalism is sometimes nothing more than the ambition of power, and many crimes have been committed in the name of universalism: historians rightfully point to the atrocities of slavery, colonialism, imperialism. At the same time, as we just did in Kabul, we dispense with universalism when it no longer suits us.

This is not a pleasant moment for a West that believed its own propaganda and thought that the collapse of the Soviet Union ushered in the triumph of Western universalism. It did not matter much if many countries, which had been the victims of European colonialism, never bought into that narrative and were always wary that humanitarian interventions were an updated version of old imperialism. The political crisis of the West and the rapid emergence of China as an example of economic success divorced from the universalist values of the West have shattered that Western self-confidence and the belief that a Western model is the future of the world. One could say that we are now irremediably shaken.

WITHER INTERVENTION?

What does all this mean for the future of intervention? One paradox of our time is that at the very moment when skepticism is growing on the wisdom of intervening forcefully in the lives of others, the rules that govern the use of force have been loosened. Unilateral interventions or interventions not sanctioned by the UN Security Council have become more frequent, and the provisions of the UN Charter on the use of force have been repeatedly violated or loosely interpreted.

This is not a pleasant moment for a West that believed its own propaganda and thought that the collapse of the Soviet Union ushered in the triumph of Western universalism.

When the 2011 Security Council resolution authorizing the use of force to protect civilians in Libya became a basis for regime change, it badly damaged the emerging norm of the Responsibility to Protect and it weakened non-proliferation efforts, as all would-be proliferators were made aware of the danger for them of renouncing nuclear weapons, as Muammar Qaddafi had a few years after the 9/11 terrorist attacks against the United States.

The response of the international community to 9/11 had even more far-reaching consequences. The Security Council radically changed the balance that the UN Charter had set when it agreed that the Al-Qaeda attacks—notwithstanding the fact that they had not been ordered or directed by the Afghan state—provided sufficient ground to launch a war against that same Afghan state on the basis of a self-defense argument: the vision of the drafters of the Charter was that authorization by the Security Council to use force would be the norm and unilateral use of force by states claiming self-defense would be the exception.

Since 2001, the unilateral use of force has become the norm, and an impotent Security Council has watched helplessly as states play an increasingly assertive role invoking the right of self-defense. There is not much confidence in the capability of a hypothetical "international community" to shape our collective future, but there is an increasing tolerance for the use of unilateral brutal force. That leaves the world in a dangerous situation: no collective will to build stability, but a higher risk of fierce unilateral responses when instability becomes a threat to national security.

Is there an alternative? This essay argues that rather than altogether abandoning the possibility of intervention, we need to do three things: *first*, define more clearly what makes an intervention legitimate; *second*, recalibrate interventions; and *third*, rethink how we intervene.

WHY LEGITIMACY MATTERS

There are indeed considerable differences between a war such as the Iraq intervention (unilaterally launched by the United States), the Afghanistan intervention (sanctioned by the UN but largely conducted by a small group of countries), the long-term deployment of troops in the Democratic Republic of Congo (sanctioned by the UN but much lighter than international deployments in Iraq or Afghanistan, yet more significant compared to even lighter deployments in other UN peacekeeping operations), and the various strictly political UN missions (characterized by a lack of international troop deployments). But they share one characteristic: even if the Afghan and Iraq wars were presented as self-defense interventions, they were wars of choice; and in that respect, they raise the same hard questions as the other two types of intervention.

The world is now in a dangerous situation: no collective will to build stability, but a higher risk of fierce unilateral responses when instability becomes a threat to national security.

Interveners need to demonstrate more rigor and honesty as they weigh the pros and cons of future interventions. What justifies intervening in the lives of others when your national security is not directly at stake? Which moral and strategic interests are at stake? What level of commitment, in both intensity and in duration, do they warrant? How assured are interveners that they will be willing and able to sustain the effort? Answering such and similar questions is the only way of addressing the question of the legitimacy of an intervention—not only in the formal sense of respect for international law, but also in its substantive dimension.

Legitimacy matters in both its formal and substantive dimensions. It matters from the standpoint of the interveners—especially if they are democracies—as they will have grave difficulties in sustaining their engagement if the intervention does not have a solid foundation accepted by a large majority.

That legitimacy should be both formal and strategic, and Afghanistan shows what happens when the strategic legitimacy of an intervention is questioned: the current Taliban regime is certainly abhorrent to many Afghans who have tasted of another way of life, but is it a threat to the rest of the world? Many experts argue that the Taliban has an essentially domestic agenda, and that, if it achieves effective control of Afghanistan, it will have little tolerance for transnational terrorist groups that could again result in devastating retaliation against the country it now controls.

What justifies intervening in the lives of others when your national security is not directly at stake? Which moral and strategic interests are at stake? What level of commitment, in both intensity and in duration, do they warrant? How assured are interveners that they will be willing and able to sustain the effort?

Of course, it is far from clear whether the Taliban will succeed in its enterprise. It may well be that a year from now, Afghanistan will have again slipped into civil war, whether because of divisions within the Taliban (between those like Haqqani network supported by Pakistan and the more independent-minded Kandahari Taliban), or because of a new challenge by enemies of the Taliban affiliated with the Northern Alliance. In either scenario, the capacity of the Taliban regime to police Afghanistan would be severely curtailed and terrorist groups based in Afghanistan could once again become a threat to other countries. But such speculative thinking had not been enough to prevent the departure of the United States in the summer of 2021.

Legitimacy also matters—perhaps even more so—in the eyes of the people of the country in which the intervention takes place. For them, formal legitimacy is essential. The divisions in the Security Council have resulted in efforts by Western countries to get around the Council's growing paralysis and write their own rules, inspired by the Christian concept of "just war."

Such past efforts may have made intervention more legitimate in the eyes of the interveners, but in the end, they are rarely enough to convince the people of the country in which the intervention is taking place: inevitably divisions within the ranks of the interveners and their political opponents feed the suspicion that the former have ulterior motives, which as a consequence undermines the trust that is required to make real progress. In the country where the intervention takes place, a lack of a broad international consensus that would have been necessary for a formal decision of the Security Council to authorize the intervention in question means that the interveners will have the gravest difficulties in building compromise—much less consensus—in the country in which they intervene. The interveners are unlikely to be seen as impartial and the intervention may

deepen divisions rather than overcome them. The disagreements over the legitimacy of launching an intervention will continue to fester after the intervention, which will in turn feed into local disputes, as we see, for instance, in Libya today.

This suggests that interventions are more likely to succeed if they are conducted in a genuinely multilateral framework, with the blessing of the United Nations, if not necessarily under its direct authority. In the present dysfunctional state of international affairs, that is likely to make intervention much rarer than in the past three decades, but there may be situations where agreement among the permanent members of the Security Council will still be possible, making intervention an option.

A combination of international divisions and national retrenchment will undoubtedly reinforce the "intervention fatigue" that prevails in the world today. But intervention should not altogether disappear from the international toolbox.

As divided as are presently the members sitting on the Council, they still agree that states are the indispensable custodians of an international order, and they are wary of a world in which spaces under the control of non-state actors expand. Thus, it stands to reason that compromise will be found somewhere between the European tradition of universalism and the Chinese vision of controlled harmony.

Calibrating Interventions

A combination of international divisions and national retrenchment will undoubtedly reinforce the "intervention fatigue" that prevails in the world today. But intervention should not altogether disappear from the international toolbox. But in order to remain a credible option, it will need to be better calibrated.

There are indeed vast differences between the deployment of a force of tens of thousands of troops supporting a multidimensional mission, the deployment of a political envoy supported by a handful of senior aides, and all the situations in between. We should abandon the illusion that the stabilization of a country broken by civil strife can be achieved quickly. More often than not, stabilization is a generational effort that requires persistence on the part of international partners. The quick entry/quick exit template, which is then followed by rapidly-held elections, simply does not work; there may be situations in which an open-ended commitment is the best option, rather than a time-bound engagement that gives the upper hand to spoilers willing to wait out an impatient or tired international community.

But the open-ended option requires calibrating the international commitment in a way that can be sustained indefinitely—an approach that is very different from what has been done since the end of the Cold War. Deciding what is the right formula will require not only having a sound evaluation of the situation, but also a willingness of international stakeholders to engage in a sustained effort.

There may also be situations in which the best option is an intense political engagement with the lightest of footprints. The war with the FARC in Colombia ended with minimal international engagement because of the traditional Latin American aversion for UN interventions, but the political support of a UN envoy and of a couple of countries that supported the process was instrumental in facilitating the conclusion of a peace agreement. The outcome of the Afghan war might have been different if, say, instead of the enormous footprint—both civilian and military—that the international community eventually came to have in the country, the role of the international community had been limited to the provision of good offices to broker an agreement between the beneficiaries of the quick war of 2001 and the Taliban.

In all situations to come, the preferred option should be the lightest possible engagement—not only for reasons of international sustainability, but also for reasons of local acceptability. There may be exceptional situations in which a strong and massive international engagement may be required for a short period of time. But such a foreign presence should not overstay its welcome. A UN flag may be better tolerated than a national flag, but in the end, any foreign presence will be perceived as an occupation, and the design of future interventions should reflect that awareness.

Rethinking Interventions

Three decades of interventions in very different contexts provide some lessons—especially on what not to do. Three lessons stand out, with each being examined in turn.

The *first* lesson has to do with in-country security. Its provision is an absolute priority in any stabilization strategy, and there is a false dichotomy between *i*) security and *ii*) service delivery/development as the foundation of legitimacy for a state trying to reassert itself in a post-conflict environment. Indeed, security is not enough; but without security, there will be no development, and there will be no effective state presence, as the populations of northern Mali have found out in villages where no civil servant wants to serve because of a credible fear of bodily harm.

The problem lies with the many flaws of the international approach to security and security sector reform. International actors see this largely as a technical undertaking in which better trained and better equipped police and military will have the upper hand. They usually underestimate the political and societal dimensions of the effort. For security forces to be effective, they need to believe in their mission and they need to enjoy the trust of the population. Both of these things depend on the political context: do soldiers and police officers respect the new authority? Do they have an "esprit de corps" that makes them proud of what they do? Are they willing to sacrifice their lives for the country they are meant to serve? Does the population see them as impartial protectors or as representatives of a particular group? Are they a threat or a reassurance?

An international presence finds itself in a trap when it has lost the capacity to transform a situation but cannot leave without risking the collapse of the country it has come to help.

Too often, these basic political conditions are ignored and the problem is aggravated by the modalities of international engagement: the international security force—whether it is an enforcement force under national command or UN peacekeepers—becomes a substitute to, rather than a support for, national efforts. It relieves national authorities of their responsibility in providing security to their people and finds itself in the uncomfortable situation of being at once rejected by the population and irreplaceable because no effective alternative force has been built, as we found out in Afghanistan.

Put differently, an international presence finds itself in a trap when it has lost the capacity to transform a situation but cannot leave without risking the collapse of the country it has come to help. Lastly, as if that was not enough, support for national efforts, when it is provided, is not always adapted to the capacities and needs of a force that will have limited resources once the international presence is withdrawn. Logistics are often provided by costly private contractors that a developing country will simply not be able to afford, while expensive and hard-to-sustain close air support becomes an indispensable tactical feature of operations.

In the future, a political understanding of the conditions for effective security should drive the international intervention effort; and the preferred course of action, in most situations, should be support to national efforts rather than substitution through the deployment of large foreign forces of peacekeepers or peace enforcers. And "support" should not become a synonym for the kind of superficial training programs that rarely help build credible forces, but rather should involve foreign officers embedded in fighting units and willing to share the same risks that the people that they are meant to support. This may limit the willingness among countries providing peacekeepers or trainers to take part in such operations; but that in itself will be a test of the seriousness of their commitment.

The *second* lesson is about state-building efforts. Everyone agrees that rebuilding a country that has been ravaged by civil strife must be a comprehensive effort, but the interventions of the last decades—whether the lavishly funded ones like Afghanistan or Iraq, or the more frugal ones like most UN multidimensional operations—have exposed the huge gap between theory and practice. Most of the time, state-building is supply-driven rather than demand-driven. National agencies, UN funds and programs, and international aid agencies and private philanthropies push their own pet projects, creating an unwieldy situation in which it is both hard to identify priorities and in which national authorities—those that international actors supposedly want to support in helping to rebuild a legitimate state—are often the spectators rather than the actors of the effort.

Moreover, the consultants and experts who design the projects often lack the anthropological knowledge that would be needed for the projects to be sustained by local chains of accountability, creating bottom-up ownership. In the absence of such ownership, there is a high risk that the offer will not correspond to the actual needs of the country in which an intervention has taken place and that the execution of the project will feed corruption rather than build a credible state. The more money, the more corruption.

Such deep flaws of state-building are hard to correct: there is just not enough knowledge to ensure that projects will be attuned to the specific characteristics of a particular country, and there is not enough discipline among the many foreign actors involved in interventions to ensure that the provision of support will follow the priorities of the country rather than those of the donors. That should not lead to abandoning any state-building efforts, however; but it should translate into us having a much more modest understanding of what can be achieved: we should consider the real rather than the assumed capacities of the international community. We should also limit our ambitions by focusing on a few priorities rather than pretending that all dimensions of state-building can be covered. If the international community is incapable of acting like a symphony orchestra. It should

test whether it can in some limited cases be a chamber orchestra.

The evolution from the "symphony orchestra" image to the "chamber orchestra" paradigm reflects the *third* and most important lesson of the past decades: the primacy of politics, and the need to subordinate all efforts to the consolidation of a fragile peace. This has implications for state-building—for instance, strengthening cabinet functions for a proper allocation of resources across the country—while building local government and accountability in parallel.

If the international community is incapable of acting like a symphony orchestra. It should test whether it can in some limited cases be a chamber orchestra.

Each situation will require a different set of priorities. But in the end, the foundation for both development and security is a political agreement that can be sustained. Without it, everything will unravel. When the international community makes the momentous decision to intervene, it should focus like a laser on the political settlement that it supports.

The next decade is likely to see less interventions than the first two decades of this century, but that newfound humility may actually lead to more successes. The world moves in cycles. In the wake of the excessive confidence of the early decades of the post-Cold War period, we have now become more cautious. This should not need lead to xenophobic retrenchment but rather to calibrated engagement.

AFTER THE AFGHAN WAR

THE U.S., RUSSIA, AND THE CHANGING SECURITY DYNAMICS IN EURASIA

Maxim A. Suchkov

THE foreign policy of the United States under the Biden Administration is developing under the influence of four factors that has been taking shape since the mid-2000s. *First*, the return of great power confrontation; *second*, the rise of a more competitive international environment (as compared to 1990s); *three*, changed American priorities in the European, Middle Eastern, and post-Soviet theaters, respectively; and *four*, the increased significance of the Indo-Pacific for American strategic, military, and economic interests.

For most of the twentieth century, the main endeavor of American strategy consisted in reshaping Europe: Western Europe after World War II and Eastern Europe after the fall of the Berlin Wall and the break-up of the Soviet Union. To achieve this goal, the United States formulated a big idea—the "transatlantic community"—and established an institution that was supposed to cement and frame this idea: the North Atlantic Treaty Organization (NATO). As a result of this effort, the United States successfully secured its military presence near one of its most important geopolitical adversaries whilst ensuring its political influence over a core group of developed states located in the Old Continent. Regardless of the various internecine disagreements that have been made manifest in the recent past, the transatlantic community still constitutes the backbone of the global American system of alliances whose significance has only increased in the new ear of rivalry with China.

The 9/11 terrorist attacks at the dawn of the twenty-first century triggered a similar attempt on part of the United States to remake the Middle East. The idea of constructing a "Greater Middle East" from Morocco to Afghanistan failed at its implementation stages,

Maxim A. Suchkov *is Acting Director of the Institute of International Studies and an Associate Professor in the Department of Applied International Analysis at MGIMO University in Moscow. He is also an affiliated expert of the Valdai Discussion Club and the Russian International Affairs Council (RIAC). You may follow him on Twitter @m_suchkov.*

Photo: Guliver Image/Getty Images

U.S. soldiers departing Kabul airport as part of the withdrawal from Afghanistan, 31 August 2021

as did numerous attempts to create some sort of "Arab NATO." The ultimate consequences of this political experiment turned out to be catastrophic for the region and still casts a haunting shadow over U.S. policymaking. In both cases—Europe and the Middle East—the official motivation behind the American push was to transform the particular part of the world from which the United States felt threatened—in the former case, the USSR; in the latter, "international terrorism"—and in so doing eliminate the very source of the respective threat.

The rapid growth of China—which has taken place simultaneous to the weakening of the international position of the United States and the deepening of America's internal crises—prompted Washington to preemptively counter the threat emanating from Beijing. This is the struggle that is likely to define the fate of the twenty-first century. Building on America's previous endeavors in Europe and the Middle East, a process of "renovating" South and East Asia is taking shape under U.S. leadership within the framework of a new big idea: the construction of the U.S.-led Indo-Pacific Region. This is now being accompanied by the establishment of security pacts and institutions designed to promote and defend the idea like

the Quadrilateral Security Dialogue (QUAD), and, more recently, AUKUS (the former is composed of America, Australia, India, and Japan; the latter of America, Australia, and the United Kingdom).

America's "playbook" for countering China is largely derived from the strategy and tactics used to contain the Soviet Union. This is only natural, since the United States has no other experience of great-power confrontation. In a similar fashion, America singles out key allies whose economic and technological potential as well as political weight and loyalty to Washington make them both the fulcrum of the American presence in respective regions and the "agents of forward containment" of the main enemy.

America's "playbook" for countering China is largely derived from the strategy and tactics used to contain the Soviet Union. This is only natural, since the United States has no other experience of great-power confrontation.

During the Cold War, such countries were Germany in the West, Japan in the East, and Turkey in the South (the latter due to geopolitical rather than economic and technological characteristics). Today, it may be Russia, the EU, India, Japan, and Australia (and to some extent South Korea) that are seen as being critical for the United States to engage in its confrontation with China. This new rivalry also requires America to concentrate more resources on its China policy, which, in turn, demands American retrenchment from some of the regions that devour too many of its resources and attention. This appears to be the logic behind Donald Trump's intention to end America's "forever wars" during his term as U.S. president. And this ended up being the logic informing the decision of his successor, Joe Biden, to withdraw America's military presence from Afghanistan.

From Counter Terrorism to Great Power Rivalry

The American departure from Afghanistan in the summer of 2021 is a case for both continuity and change in American politics. The decision to leave Afghanistan was made long before Biden came to office—the Forty-Seventh President of the United States just executed the decision his predecessors had sought yet failed to implement for various reasons. As an outside observer of American politics, it strikes me that Biden's 31 August 2021 address announcing the "end of the war in Afghanistan" could easily have been delivered, for the most part, by his predecessor. Much of the speech was about national egoism; little was devoted to explicating the responsibilities of a superpower.

This attitude is nevertheless understandable: the U.S. has long been experiencing "Afghanistan fatigue" and most American citizens have no regrets in having left the turmoil behind. But it also shows that just like past U.S. president, Biden operates in three primary capacities concurrently: as a party politician, as a manager of a large bureaucracy, and as a military commander-in-chief.

As a politician, his primary interest is to maximize the chances for his party to win the next elections—both for the U.S. Congress and the executive office. Although it is too early to assess the prospects for the Democrat Party on this subject, the withdrawal from Afghanistan is unlikely to impact on voter preferences. The Republican Party will certainly try to make the most of this situation by playing the Biden's lame leadership" card to its fullest. Still, the Afghanistan story arc is unlikely to play a large role in whether the Democrats lose or win the 2022 midterms or the 2024 presidential race. There are a lot more important issues for American voters, including the state of the economy, rising inflation, heightened spending on infrastructure, illegal migration, and various pandemic-related issues. The battle for American high offices is most likely to be won or lost on these fronts.

Biden's decision to withdraw from Afghanistan truly ended an era that began with 9/11. The fight against terrorism is no longer the defining paradigm of American security and foreign policy.

Biden may have failed as a manager of bureaucracy: the pullout from Afghanistan appeared to have been poorly coordinated and awfully executed. But in that particular decision chain, his thinking was most probably dominated by his third role—that of commander-in-chief.

In this last capacity, Biden's decision to withdraw from Afghanistan truly ended an era that began with 9/11. The fight against terrorism is no longer the defining paradigm of American security and foreign policy. The United States is moving—or returning—to a great-power standoff with China and, partly, Russia. Many in Washington believe it is the fight that will determine the fate of humanity in the twenty-first century. Moreover, by withdrawing the American military contingent, the United States does not intend to reduce its intelligence capabilities in the region. On the contrary, the Americans are now championing amongst themselves the need to deploy additional intelligence resources in adjacent territories under the official pretext of monitoring possible terrorist activity in Afghanistan and tracking the character of the Taliban's relations with other Islamists.

But such an intelligence infrastructure, many in Russia fear, will also come in handy for that very "great-power confrontation" with both Russia and China in a zone that is, in terms of security matters, sensitive for all three.

FORWARD TO THE PAST

For Russia and much of Eurasia, the second advent of the Taliban suggests that the topic of combating terrorism has found its way back to the top of the agenda. To make matters worse, the advanced weaponry the Americans left in Afghanistan could hypothetically make a future fight with the Taliban more technologically challenging. Unlike Washington, which feels it can now afford to not see counter-terrorism activity as a framing paradigm of its security, Moscow does not have this luxury—Afghanistan is only 3,367 km away from the Russian border.

That the Taliban and ISIS-K predate on different theological, philosophical, and political "schools" is known and is of interest only to a handful of academics. For ordinary people, including young people with a "exacerbated Islamist identity," "it makes no difference what color a cat is as long as it catches mice," as Deng Xiaoping once put it.

Certainly, the topic of combating terrorism has never ceased to be relevant for Moscow. But the very victory of the Islamists and the re-creation of the Islamic Emirate is a very dangerous signal to likeminded extremists around the world. That the Taliban and ISIS-K predate on different theological, philosophical, and political "schools" is known and is of interest only to a handful of academics. For ordinary people, including young people with a "exacerbated Islamist identity," "it makes no difference what color a cat is as long as it catches mice," as Deng Xiaoping once put it. In other words, for the majority of Islamists out there, the message that the Taliban victory may be sending is this: what didn't work out in Iraq and Syria will work in Afghanistan. It is less important in this regard that the Taliban have a different model of state-building than what ISIS propagates, or that the Taliban use different slogans, or that they are a local movement and not a global one. The bottom line is that they represent a success story that dozens of radical groups around the globe may be tempted to repeat.

Therefore, reasonable concerns for Russian policymakers are that these "sleeper cells" of radicalism may be reawakened once again in certain Russian regions and in parts of Central Asia as well. Hibernating terrorists are not just a Eurasian problem, as evidenced by multiple terrorist attacks on the territory of the European Union over the past few years. It is also clear that the long-promoted battle against this phenomenon is not possible without a form of cooperation based on a unity of efforts: a cooperation that does not tolerate the ambiguity of state willpowers towards acting in concert, a cooperation that transcends political divisions, and a cooperation that does not cloud common sense in assessing real threats.

In the fight against terrorism, Western counterparts, with rare exceptions, shy away from cooperation with Moscow.

Yet, the prevalent mood in Moscow at the moment is that cooperation in this area with Western countries, though still desirable, seems unlikely after decades of failed attempts to establish a modus for doing so. In the fight against terrorism, Western counterparts, with rare exceptions, shy away from cooperation with Moscow.

Moscow therefore sees the current situation as a window of opportunity to boost its security cooperation in the field of counter-terrorism (and beyond) with major non-Western states that also may be alarmed by the arrival of the Taliban: China, India, and to some extent Iran—not to mention Russia's Central Asian partners in the Collective Security Treaty Organization (CSTO).

The new situation will require Moscow to exert more resources and focus on its domestic political situation as well as its "near abroad." Yet, on the external circuit, what we can call the "overheating" of the Russian frontier can be avoided by "managing responsibility" with allied countries whilst concurrently conducting delicate diplomacy with respect to relations with the Taliban. For the moment, the Taliban look cooperative. Yet with more power comes the appetite for ideological expansion and purposeful geopolitical adventures; so this movement will need to be kept in check.

SURVIVAL GUIDE

Less than two months before the United States left Afghanistan (on 9 July 2021, to be precise), Moscow hosted a delegation of the Taliban's Doha-based "political wing." The outcome of these negotiations represent the key to understanding Russia's subsequent actions towards the Taliban, for those talks laid out the basis for Russia's *modus operandi* with the movement.

The conversation basically revolved around four key areas. *One*, eradicating security threats to Russia and its Central Asian allies that might originate from Afghan territory; *two*, preventing

potential instability spillover to Central Asia; *three*, curbing the drugs trafficking route from Afghanistan through Central Asia to Russia and further onwards to the European Union; and *four*, providing for the safety of Russia's diplomatic mission.

Moscow had few illusions about the nature of the Taliban, which Russia designated as a terrorist organization in the early 2000s when President Vladimir Putin agreed to an American request to open up Russian territory to NATO's wartime logistical efforts in the Afghanistan theatre. Yet now that the Taliban have assumed responsibility and provided guarantees with respect to each of the aforementioned four items, the name of the game has become different on the basis of classical Realpolitik principles.

The Russian leadership conducted itself on the considered premise that that the Taliban's back-channel diplomacy with Beijing and Tehran, together with its the shuttle diplomacy with Moscow and Washington (or, rather, Doha), was meant to establish a calm external environment that would provide the Taliban with enough time, a form of de facto legitimacy, and, ideally, sufficient resources to consolidate its hold on the levers of power in Afghanistan. In other words, the Taliban was believed to have had its own incentives to make credible commitments to the Kremlin with respect to the Moscow's chief priorities in the area: border security, stability in the "near abroad," and ensuring the safety of its diplomats.

That being said, even if the Taliban do not mean to execute its commitments in full (of if it is incapable of doing so for whatever reason), Russia basically has no other option to deal with the movement. Over the past few years, the Russian military and the country's economy have been overstretched along multiple fronts: from Ukraine and Syria to Libya and Karabakh. While Russia's own posture in its talks with the Taliban is underpinned by modern-day military capabilities that the Soviets simply did not possess in the 1970s and 1980s, the Soviet fiasco in Afghanistan is a public memory that serves as deterrent against any significant physical intrusion into Afghanistan.

Therefore, following the snap American departure, Afghanistan emerged for Moscow as yet another unnecessary distraction—and not as a "vacuum to fill," as many in Washington presumed. Still, because stability in Central Asia and the overall security of Russia's southern flank are in effect conjoined to the theme of extremist ideologies—reportedly one of Putin's favorite subjects—the issue is front and center on the Kremlin's radar screen. This combination of the factors, coupled with the Taliban's willingness to negotiate a "non-conflict mode of co-existence," provided Moscow with the opportunity to establish concrete red lines with the Taliban.

This being the case, the Kremlin pursued what now appears to be a double-track approach. On the one hand, Moscow has been talking to the Taliban via diplomatic channels. On the other, Russia has been conducting joint military drills with Uzbek and Tajik troops while also beefing up the military of its CSTO allies. Interestingly enough, the military exercises have been operating under the slogan of a "joint response to cross-border militant attacks"—which is also a clear message to the Taliban. The drills have involved tanks, armored personnel carriers, helicopters, SU-25 attack jets, and other advanced weaponry.

Therefore, following the snap American departure, Afghanistan emerged for Moscow as yet another unnecessary distraction—and not as a "vacuum to fill," as many in Washington presumed.

Russia cannot be happy with the fact that an Islamic Emirate stands close to it border. Yet, as long as the Taliban observes the aforementioned four-item "agreement" and keep its Islamist agenda local—as bad as it may be for Afghanistan—Russia believes it can tolerate its presence in the neighborhood. Having this new neighbor would imply a more intense life for Russian security services and law enforcement. For instance, the Defense Ministry will have to do a lot more military coordination with its Central Asia peers; Russia's military intelligence (GRU) will be kept busy monitoring the situation; the Federal Security Services (FSB) will be preoccupied with tracking possibly rising Islamist influences in Central Asia and Russia; and the Federal Drug Control Service will be put on high alert for potential new heroin production schemes and flows to Russia. But even under these circumstances, diplomatic engagement still appears a better option for Russia than getting involved militarily with no clear political goals or an exit strategy.

VEGAS RULES

For Russia the present situation in Afghanistan is actually about both Afghanistan and the United States. Mainstream Russian political and expert discourse suggests that Moscow is as concerned about the security of Central Asia as it is critical of the 20-year presence of the U.S.-led coalition in that country.

The bottom-line of that criticism is the ultimate failure of the United States to build both an effective Afghan military able to defend against the Taliban and a "nation" that wouldn't fall apart

under the terrorist offensive. The crumbled Afghan statehood is thus portrayed by Russian policymaking community as a direct consequence of America's strategic blunders. This argument is further projected onto countries like Ukraine and Georgia and other actors, like Russia's own opposition groups which, in the Kremlin's view, rely too much on the American support. Moscow is now embedding the reasoning of "not only will the Americans not help you, but they will likely make things worse" into its persuasion tactics with the leaderships of these countries and these groups to have them change their respective calculus on dealing with Moscow, since only Moscow, not Washington, "means business." In a nutshell, the Afghan story is seen in Moscow as an opportunity to further "de-Americanize" the international system and Russia is intent to make the most of it.

The crumbled Afghan statehood is thus portrayed by Russian policymaking community as a direct consequence of America's strategic blunders. This argument is further projected onto countries like Ukraine and Georgia and other actors.

For now, Russia has adopted a wait-and-see approach in Afghanistan. It seeks to engage with key regional stakeholders and is stressing the need for greater regional cooperation within the CSTO and the Shanghai Cooperation Organization. In Russia's vision, there's minimum, if any, role for the West to play.

"The problem is that in the Mideast the Las Vegas Rules don't apply. What happens in the Mideast doesn't stay in the Mideast." This quote by David Petraeus, a former CIA director and commander of the International Security Assistance Force (ISAF) in Afghanistan, is not just a wise observation on the essence of the 'politics of the East.' It is also an edification to the political leadership of the United States—both Republicans and Democrats—that events in regions like the Middle East or South Asia often have consequences that at once go far beyond narrowly-conceived geographical boundaries as well as transcend political cycles. This quote should also be understood as advice to Washington—as much as to any other capital from Moscow to Beijing—to approach decisionmaking with respect to complex regions in a more balanced and nuanced way. The distinguished general who implemented political decisions made by American politicians in the vastness of Iraq and Afghanistan put a deep meaning into this metaphor, and his political descendants better read more into it than they have so far.

HORIZONS
Discussion

Building Forward Better: After the Rain

On 16 September 2021, renowned historian and Horizons author ***Niall Ferguson*** *joined CIRSD President* ***Vuk Jeremić*** *in a wide-ranging, no-holds-barred online discussion about the issues raised in his essay as well as in those raised by other distinguished contributors—leading thinkers of our time—including* ***Jacques Attali***, ***Alan M. Dershowitz***, ***Jeffrey D. Sachs***, ***Nouriel Roubini***, *and* ***Thierry de Montbrial***.

LESSONS LEARNED IN AFGHANISTAN

A PRELIMINARY ASSESSMENT

Dov S. Zakheim

IT will be some time before the United States, its NATO allies, and other partners that contributed troops and/or resources to the effort to rebuild Afghanistan will be in a position to assess all the implications of the failure of that effort. What follows, therefore, is a preliminary assessment that no doubt will have to be modified to some extent as more facts emerge to explain why an operation that bore so much promise in the first years of the new century turned out to be such a spectacular disappointment two decades later.

Perhaps the first indication that all was not well with what was called Operation Enduring Freedom was the failure to capture Osama bin Laden. The leader of al-Qaida managed to escape from Tora Bora in December 2001 because fewer than 100 American commandos were on the scene with their Afghan allies while calls for reinforcements to launch an assault fell on deaf ears. So too did requests for American troops to block bin Laden's escape route to Pakistan. As a result, he and his bodyguards simply walked out of Tora Bora and were able to hide in Pakistan's tribal area in order to continue their fight against the West. The episode highlights the dangers of over-emphasizing initial success before an operation is truly complete.

Early in 2003 Washington launched its ill-fated attack on Saddam Hussein's Iraq. Unlike its attack on the Taliban, it did so without the support of several key allies, notably France, Germany, and Canada. Like the initial phases of the Afghanistan operation, Operation Iraqi Freedom was a smashing success. Yet even before America and its coalition were bogged down in Iraq, the very move to launch a second war undermined the likelihood of success in Afghanistan. Key American civilian officials and top military personnel refocused their attention from Afghanistan to Iraq, and with that shift in focus came a shift in resources as well. By relegating Afghanistan to the back burner, Washington enabled the Taliban to regroup in their Pakistani hideaway.

Photo: Guliver Image/Getty Images

Members of the Taliban enjoying the fruits of Kabul's reconquest, 20 September 2021

Even as it shifted focus from Afghanistan, Washington engaged in yet another of its many attempts at nation-building. This effort fared no better than its previous undertakings in places like Haiti, Somalia, or the Balkans. The nation-building enterprise called for what is termed a "whole of government approach." Yet all too often it was left to America's armed forces to lead the effort by default, a task for which they simply are not suited. Other government agencies often simply did not have sufficient numbers of trained and experienced personnel to undertake the multiplicity of tasks that nation-building demanded. On the other hand, military service personnel were unfamiliar with local culture and mores. Their ignorance at times resulted in engendering hostility among the very people they were meant to support. Troops and their senior officers rotated in and out of Afghanistan far too often to obtain a deep understanding of the country or, for that matter, to develop serious relationships with its people.

Dov S. Zakheim *Dov S. Zakheim was an Under Secretary of Defense in the first George W. Bush Administration and a Deputy Under Secretary of Defense in the second Reagan Administration. He is currently a Senior Adviser at the Center for Strategic and International Studies.*

As a result, they had difficulty developing any real traction with the people of Afghanistan.

Successive administrations acted on the premise that Afghanistan could be transformed from a feudal society that had remained virtually unchanged for centuries into a modern state. The unpleasant reality that Washington and its allies refused to accept was that what they viewed as progress, conservative Afghans—particularly in the countryside—considered to be a threat to their way of life. The results have proved tragic. In particular, whatever progress women had made over the course of two decades was shattered in a matter of weeks by a Taliban government determined to restore male dominance over all facets of life in Afghanistan.

Even as it shifted focus from Afghanistan, Washington engaged in yet another of its many attempts at nation-building. This effort fared no better than its previous undertakings in places like Haiti, Somalia, or the Balkans.

Prior to 9/11, George W. Bush had made clear his distaste for nation-building. His successor, Barack Obama, argued for "nation-building at home." Obama's successor, Donald Trump, was of a similar view, as is current U.S. president Joe Biden today. One would hope that America finally learns that other nations may well be better suited to the complicated enterprise that is nation-building.

The failure of "whole of government" to function properly also was a major factor in the chaos that ensued at Hamid Karzai International Airport during the final days of the American withdrawal. The linkup between the military operating inside the airport and at its entrance and the State Department personnel who functioned outside the airport was tenuous at best. Instead, successful cooperation depended heavily on selfless efforts by some officials from both the State Department and the Department of Defense took the initiative to assist Americans and Afghans desperate to leave the country. It is therefore high time that "whole of government" no longer remain a buzzword but rather, and at long last, become standard operating procedure for the United States government.

Washington provided far too little careful oversight of the many contractors that operated in support of the American and Afghan forces. As long as a decade ago, it was clear that the fault lay not with the contractors, but with the United States government. I served on the Commission on Wartime Contracting in Iraq and Afghanistan, which the U.S. Congress had mandated

in 2008 and that reported its findings three years later. Initially, a few of my fellow commissioners were inclined to blame the contractors for whatever waste or fraud that the Commission would unearth. As we investigated the situation on the ground in both countries over the course of nearly two years, we found that the government itself was primarily at fault for waste that we estimated totaled anywhere from $31 to $60 billion (equivalent to approximately 37 to more than 71 billion in fiscal year 2021 dollars) as a result of poor government oversight, unclear specifications, mindless automatic contract renewals, and lack of transparency into subcontractor costs.

Washington provided far too little careful oversight of the many contractors that operated in support of the American and Afghan forces.

One example of the Commission's findings foreshadowed the ultimate collapse of Afghan security a decade later. The Commission reported that "between FY 2006 and FY 2011, Congress appropriated $38.6 billion, an average of $6.4 billion a year, to the Combined Security Transition Command- Afghanistan (CSTC-A) program to train, equip, and provide other support for the Afghan National Security Forces (ANSF). Such costs far exceed what the government of Afghanistan can sustain." The Commission could not identify where the monies had actually gone.

Reports that the Special Inspector General for Afghanistan Reconstruction published subsequent to the Commission's findings highlighted additional wasted funds. Indeed, shortly before the collapse of President Ashraf Ghani's government in Kabul, the Special Inspector General published yet another report that stated that Washington had spent $83 billion over the past 20 years to build the ANSF. How much of that massive sum went to waste has yet to be determined. Nevertheless, it is undeniable that the U.S. government's mismanagement of its contractors and contracts ate away at its efforts to stabilize Afghanistan and restructure its military. Equally undeniable is the fact that many if not most of the recommendations that both the Commission and the Special Inspector General put forward for at least a decade, and to which the Department of Defense paid lip service, never were implemented.

Moreover, contractors never really handed over to Afghans the responsibility for maintaining and supporting the many weapons and weapons systems that the United States had transferred to the Afghan National Defense Forces over the course of two decades. Washington never insisted on any timetable for contractors to complete their training and

maintenance missions so as to enable the Afghan forces, and especially the air forces that were so critical to keeping the Taliban at bay, to operate on their own. As a result, when American forces departed from Afghanistan in August 2021, the Afghan military personnel were unable to operate many of the systems that they had acquired. In particular, Afghan inability to support flying operations effectively grounded the Afghan Air Force, which probably constituted the most powerful capability that the Kabul government could marshal against the Taliban.

The Obama Administration made a deliberate choice to focus on nation-building and to ignore the reality that corruption ultimately would undermine not only its reconstruction efforts but also the fighting capacity of the Afghan forces.

Here, too, there is a lesson to be learned. Not only should the U.S. Government tighten its contracting procedures, but it should also ensure that contractors do not permanently retain a monopoly on the support and maintenance of systems that Washington transfers to its allies. In particular, the government should insert into its contracts deadlines by which time contractors should have fully trained allies that receive American equipment. These contracts should explicitly state that failure to execute such a requirement would result in what is termed "termination by default," meaning that the contract would be cancelled with no resulting government liability for doing so.

By 2011, it also was clear that the Afghan government was riddled with corruption. The withdrawal of American forces from Afghanistan and the Taliban's lightning victories initially in its attacks on the various provincial capitals and then on Kabul itself underscored the impact of corruption on the collapse of the Afghan National Defense and the consequent fall of the Afghan government. Afghan military morale had plummeted as troops went months without pay, without basic essentials, and even without food. And the lower ranks were fully aware that their seniors were embezzling funds and supplies.

Moreover, the corruption at the level of both the government in Kabul and various provincial governments was an open secret. American political and military leaders had been given due warning for more than a decade. The reports of the Special Inspector General for Afghanistan noted scandal after scandal. Some made headlines, like the 2010 Kabul Bank scandal. Others received far less publicity but were no less secret. For example, it did not require intelligence agencies to track where huge sums of American aid money, or, for that matter, illicit drug money, were going. For years it was widely known that senior Afghan leaders, among them some of the most senior ministers, had siphoned off funds that they employed to acquire estates in Dubai, in particular, and other similar places.

Washington's manifest over-eagerness to leave the country simply led to its capitulating to the Taliban's refusal to deal directly with the Kabul government.

As Sarah Chayes, a journalist who spent a decade in Afghanistan has reported, the Obama Administration made a deliberate choice to focus on nation-building and to ignore the reality that corruption ultimately would undermine not only its reconstruction efforts but also the fighting capacity of the Afghan forces. Four decades earlier, American administrations overlooked the analogous reality that South Vietnamese government corruption had undermined its military's morale and willingness to fight. America repeated the same mistake in Afghanistan; it should not do so again.

In perhaps what was one of Washington's gravest errors, the Trump Administration chose to negotiate with a non-state actor—the Taliban—while excluding the legitimate Afghan government. It was always questionable why it elected to do so. It is difficult to accept assertions that there was an arrangement whereby the Kabul government would be brought into the negotiations at a later date. Washington's manifest over-eagerness to leave the country simply led to its capitulating to the Taliban's refusal to deal directly with the Kabul government. In so doing, America permanently undermined the government's credibility with its own people. It is a mistake that Washington should not repeat.

The Biden Administration's chaotic exit from Afghanistan involved numerous errors, some of which also provide lessons for the future. To begin with, it misled itself into believing that the Taliban would abide by the terms of the Trump-negotiated February 2020 Doha agreement, which it had advertised as the first step in a process that would lead both to American and NATO withdrawal of their forces and a settlement between the Taliban and the Afghan Government. The agreement was an awful piece of negotiation. It was lopsided in favor of the Taliban, which was not even a state and was referred to in the agreement as "the Islamic Emirate of Afghanistan which is not recognized by the United States as a state and is known as the Taliban." For its part, the United States committed itself to withdrawing all is forces from Afghanistan and closing all Coalition bases in that

country within 14 months, that is, by the beginning of May 2021. It promised to reduce its forces in Afghanistan to 8,600 and, together with its allies, to withdraw from five military bases by mid-June 2020. Finally, in what the agreement termed "a confidence-building measure" it provided that "up to five thousand (5,000) prisoners of the Islamic Emirate of Afghanistan which is not recognized by the United States as a state and is known as the Taliban and up to one thousand (1,000) prisoners of the other side will be released by March 10, 2020, the first day of intra-Afghan negotiations."

For its part, the Taliban did not commit to very much. Its primary undertaking was to engage in "intra-Afghan dialogue and negotiations." These negotiations were never serious, however. The Taliban had no incentive to cooperate with a government that it had refused to recognize and deeply despised. Washington had yielded to the Taliban by freezing the Ghani government—the country's legitimate and internationally recognized government—out of both the negotiations and the agreement. As some sort of consolation prize, Washington promised to bring the government into the discussions at some unspecified future date. It was hardly surprising that ordinary Afghans could only conclude that Washington had *de facto* recognized the Taliban and at the same time had ignored what was meant to be its ally and the legitimate government in Kabul. The result was Taliban anticipation of victory and a demoralized Afghan military.

Despite the Taliban's clear breach of its commitments, for some reason, however, it appears that the Biden Administration felt that it could "do business" with the Taliban.

Moreover, in a manner reminiscent of General Vo Nguyen Giap's ultimately successful offensives against the Army of [South] Vietnam (accelerated after the seemingly successful negotiations that led to the 1973 Paris Accords), the Taliban intensified its operations against the Kabul government's forces throughout the country in the aftermath of the agreement. Additionally, once the Afghan government under pressure from the Trump Administration released 5,000 prisoners, many of them simply rejoined the Taliban's forces.

Despite the Taliban's clear breach of its commitments, for some reason, however, it appears that the Biden Administration felt that it could "do business" with the Taliban. When it took office, it need not have clung to the agreement negotiated by its predecessor. The Taliban was still attacking Afghan forces. It was not negotiating in good faith. Yet Biden chose not only to adhere to the Doha Agreement, but to retain America's negotiator, Zalmay Khalilzad. Yet having negotiated the Doha Agreement, Khalilzad could not be expected either to seek its modification, or to renounce it. As a result, rather than reneging on the Trump Administration's deal with the insurgents, for which Washington would have been fully justified, the Biden team instead adhered to the agreement, arguing that it had little choice to do otherwise, though Biden had not hesitated to rescind numerous Executive Orders that Trump had issued on a whole host of other issues.

Washington also succumbed to a degree of self-delusion reminiscent of the Pentagon's baseless optimism as it became increasingly clear that the Vietnam War could not be won. Even as provincial capitals were falling to the Taliban in the spring and summer of 2021, the Biden Administration seemed convinced that the Afghan government's forces somehow would manage to hold off the Taliban at least for several months without American support. When those forces collapsed, American officials acknowledged that they had miscalculated the speed with which Afghan forces collapsed before the Taliban's onslaught.

When Biden announced that he was extending the deadline for American withdrawal to September 11, 2021, so as to mark the completion of the twenty years' war that had begun on that date, he did not order his subordinates to speed up the process of extracting Americans and their Afghan allies and supporters out of the country. Biden excused his failure to do so on the grounds that his Afghan counterpart, Ashraf Ghani, had pleaded with him not to publicize an evacuation, since it would undermine Kabul's credibility and authority. By then, however, Kabul had neither credibility nor much authority. Its forces were being soundly defeated throughout the country. Its government was widely viewed as corrupt to the core. The government's jurisdiction barely extended beyond Kabul as provincial capitals began to fall. Yet Biden did not order a full-scale evacuation until the Taliban was at Kabul's gates. Interestingly, France and other coalition partners that no longer had troops remaining in Afghanistan acted far more quickly to extract its own personnel from the country.

Biden Administration officials also erred in withdrawing forces from the large Bagram Air Base whose two runways would have smoothed the exodus of American and Afghan personnel in the final days of August 2021. Biden Administration spokesmen continue to insist that they could not have protected Bagram from the Taliban, since it would have taken 5,000 troops to do so—far fewer than were available throughout the country. The Biden Administration also insisted that it could not have provided protection for Americans and Afghans seeking to flee to Bagram,

since the Taliban would have targeted the roads to the airbase, which is some 36 miles from Kabul.

Both assertions are open to question, however. To begin with, testifying before the Senate Armed Services Committee on September 28, 2021, General Mark Milley, Chairman of the Joint Chief of Staff, stated that his view was that "we should keep a stead state of 2,500 [troops in Afghanistan] and it could bounce up to 3,500." Similarly, General Kenneth McKenzie, commander of Central Command, told the committee that he had also recommended that the United States retain 2,500 troops in Afghanistan to support the government's troops. Presumably, if those forces sufficed for the entire country, they surely would have proved sufficient for protecting Bagram. Moreover, retaining Bagram would also have enabled American fighters to provide air cover to protect people seeking to flee Kabul and other parts of the country from attacks by the Taliban. And it is unclear whether the Taliban would have attempted to prevent those fleeing the country so long as it would be clear that American military forces were departing as well.

Biden provided his NATO allies and others who had joined the coalition to fight the Taliban little to no notice that it was withdrawing from the country at the end of August 2021 rather than on September 11, as he had previously announced. These countries were caught flat-footed and if, like France, they had not already done so, scrambled to get their people out of Afghanistan even as Kabul was falling. As a result, it further intensified a growing concern among allies and partners about Washington's reliability.

Trump now appears to be no more than an extreme expression of what Americans have come to feel about their country's role in the world.

The challenge that America's friends face is that the United States appears to be undergoing a serious change for the worse. It no longer radiates the same degree of solid commitment to preserving the international order—which it had actually constructed— as has been the case since the end of World War II. It has not been lost on foreign observers during the 2016 presidential primary campaign that the four candidates who remained in the race—Donald Trump, Hillary Clinton, Ted Cruz, and Bernie Sanders—all opposed expanding America's free trade policies, a sure sign that America was increasingly looking inward.

It was nevertheless arguable, at least during Trump's tenure, that his isolationist impulses—withdrawing from both the Trans-Pacific Partnership (TPP) and the Paris Climate Accords, threatening to leave NATO, raising new tariffs barriers, and of course, pressing for America's withdrawal from Afghanistan—were an aberration. Yet in addition to presiding over America's departure from Afghanistan, Biden has neither removed Trump's tariffs nor joined the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the successor to the TPP. Trump now appears to be no more than an extreme expression of what Americans have come to feel about their country's role in the world. And America's allies and friends therefore are hedging their bets regarding America's reliability, with Europeans taking greater interest in French President Emmanuel Macron's case for "strategic autonomy" and various Middle Eastern states—Gulf Arabs and Israel alike—maintaining and in some cases intensifying their relations with China and Russia, countries that Washington now designates as its "peer competitors."

Ironically, as America confronts threats from China and Russia, it does so with a far smaller force structure than it maintained during the Cold War; for that reason, it finds itself far more dependent on its allies and friends than at any time since the Revolutionary War. The Biden Administration must therefore be far more responsive to allied sensitivities. In that regard, the recent flap over the surprise cancellation of the French Barracuda conventional submarine program in favor of a new American-British-Australian effort to produce nuclear powered submarines has been less than helpful.

Finally, the exit from Afghanistan has created a vacuum that China appears quite eager to fill. Just a few weeks before the United States departed from the country, nine Taliban leaders, including Mullah Abdul Ghani Baradar, currently the acting first deputy prime minister of the reconstituted "Islamic Emirate of Afghanistan," met in Tianjin with Chinese Foreign Minister Wang Yi at China's invitation. Wang spoke approvingly of the Taliban, calling the group "a pivotal political and military force" in Afghanistan. Working together with its long-time ally Pakistan, which served as the Taliban's base during the war with the United States, China clearly will be a major player, especially in the economic realm, now that the Taliban has returned to power.

This outcome represents yet another aspect of what can only be termed America's defeat in Afghanistan. Given China's ambition to restructure the world economic order, Washington must do all it can to avoid other mistakes that will give Beijing the economic opportunities it so doggedly seeks.

There no doubt will be many more lessons to be gleaned from a thorough review of America's Afghan misadventure. Nevertheless, to the extent those outlined above seem likely to withstand the test of time, Washington should not hesitate to act upon them as soon as it possibly can.

Hope Against Hope in Afghanistan

James M. Dorsey

FEW in the international community, including Afghanistan's neighbors and near-neighbors, are holding their breath that the Taliban will make good on their promises to respect human, women's, and minority rights, uphold freedom of the press, and appoint a more permanent, truly inclusive government.

Hopes for Taliban cooperation with the international community are perhaps highest when it comes to the group's pledge to police militants on Afghan soil and ensure that they do not launch cross-border or transnational attacks. Yet, even there, the Taliban's track record is chequered, notwithstanding the fact that the group only recently took control of Afghanistan. The record already casts doubt on the Taliban's willingness and ability to impose its will on various militant groups. So does the Taliban's failure to capitalize on its fight against the Islamic State's Central and South Asian affiliate, Islamic State-Khorasan Province (IS-K), as well as IS-K's brutal campaign against minority Hazara Shiites.

A Three-Pronged Approach

Armed Taliban fighters in captured police pickups showed up in early September 2021 in remote Shiite villages in the Tagabdar Valley in the central Afghan province of Daykundi. They summoned the villages' men to issue an ultimatum: they and their families had two weeks to leave their villages. According to *Der Spiegel* journalists Christoph Reuter and Thore Schroeder, the fighters warned the villagers that deadly force would be used if they did not leave voluntarily. The villagers were served with a notice from the governor of Daykundi informing them that they must leave their lands.

"But where are we to go?" one of the men summoned by the Taliban asked.

James M. Dorsey *is a Senior Fellow at the National University of Singapore's Middle East Institute and the author of the syndicated column and blog, "The Turbulent World of Middle East Soccer." You may follow him on Twitter @mideastsoccer.*

"Doesn't matter," the Taliban answered, "just depart this Garden of Eden surrounded by an inhospitable landscape." Many of the hundreds of families forced to leave had nowhere to go, including Jamilah, a 45-year-old widow, who lives out in the open with her six children since leaving home. They are exposed to the elements, with little food or water. "Now, we are forced to sleep in the open. We are hungry and thirsty. What will we do when it's winter?," she told Ghandara, an online news service.

The villagers had good reason to take the Taliban threat seriously. Hazara Shiites, who account for 20 percent of the Afghan population, had not fared well during the Taliban's first stab at government in the 1990s, until they were swept from power by the 2011 U.S. invasion of Afghanistan. The Taliban, like jihadists and other Sunni ultra-conservatives, view Shiites as heretics. Hazaras have warned for months that a renewed Taliban takeover posed an existential threat to their community.

Even worse, IS suicide bombings of Shiite mosques in Kunduz in the north and Kandahar—the Taliban's heartland in the south—two months after the forced evacuations in Daykundi, suggested that the Hazara were caught in a pincer movement by two sworn enemies. The Islamic State, in a rare move apparently designed to capture China's attention and complicate relations between the Taliban and Beijing, disclosed the ethnicity of the perpetrator of the Kunduz attack, saying he was an Uyghur. By the same token, the attack was likely to cast a shadow over efforts to forge a working relationship by both the Taliban and Iran, which views itself as the protector of the Shiite Muslim world.

Taken together, the bombing and the evacuations indicated that the fight with the Islamic State would in part be fought over the backs of Shiites. The attacks raise the question of whether the Taliban's effort to control jihadists and other militants operating on Afghan soil amount to more than a dogfight between equally bad alternatives. They also raise the specter of Iranian failures to find a *modus vivendi* with the Taliban because of its inability to protect Shiites.

The evacuations, a potential prelude to ethnic cleansing, belied the notion of a Taliban 2.0 that was supposed to be more inclusive and empathetic to others' rights. They were the side of the coin the Taliban preferred to keep out of sight. Taliban protection of recent Shiite religious celebrations may have been equally sincere but served the purpose of promoting the image of a more moderate and gentler Taliban.

That is not to say that the effort to control other militants is not serious and perhaps as existential to the Taliban as is the threat Hazara Shiites

are facing. For much of the international community that has *de facto* accepted Taliban rule, the determining factor for *de jure* recognition is likely to be the Taliban's ability to prevent militants from using Afghanistan as a launching pad for cross-border or trans-national attacks.

As a result, the Taliban developed a multi-pronged strategy involving confrontation of the Islamic State that opposes Taliban rule because the group was willing to negotiate with the United States; negotiations with various other militant groups, including Al-Qaeda, that have produced at best-mixed results; and reliance on a potential paradigm shift in jihadist strategy away from transnational attacks and towards local governance.

For much of the international community that has de facto accepted Taliban rule, the determining factor for de jure recognition is likely to be the Taliban's ability to prevent militants from using Afghanistan as a launching pad for cross-border or trans-national attacks.

Consider in this context the Islamic State-Khorasan Province, at this point the Taliban's most formidable opponent as a result of having demonstrated credibly its potency inside Afghanistan. The Kunduz and Kandahar bombings followed the attack on Kabul airport that killed 13 U.S. soldiers and 169 Afghans as the United States was evacuating the countries. The Islamic State has since also launched multiple smaller-scale attacks, including assassinations, kidnappings and beheadings of Taliban fighters on patrol.

Violence is one aspect of the group's methodical, multi-faceted strategy that also involves reaching out to tribes and other groups, stamping out dissent among more moderate Salafis and carrying out jailbreaks, assassinations, and attacks on Taliban personnel. "Package all of that together, that is an entire method of insurgency the Taliban is not equipped to handle," said extremism scholar Andrew Mines. Tens of tit-for-tat killings in Nangarhar, an IS stronghold, illustrate the Taliban's difficulty to impose law and order—a cornerstone of its appeal throughout the group's history.

The Taliban botched an opportunity to inspire confidence when acting Afghan interior minister Sirajuddin Haqqani convened family members of Taliban suicide bombers to celebrate the actions of their loved ones. Rather than apologizing to the victims, Haqqani—who has a $10 million bounty on his head due to close ties with Al-Qaeda—told the gathering that the bombers' "sacrifices are for religion, for the country, and Islam." Ironically enough, the gathering took place in Kabul's Intercontinental Hotel, which was twice targeted by the group. He added that the Taliban would not have been able to fight the United States without the support of suicide bombers.

Doubts about the Taliban's ability and willingness to live up to its promises are fed even more by the composition of the group's caretaker government, which includes multiple figures designated by the UN and/or the U.S. as terrorists. The concern is not limited to the notorious Haqqani family, but also other members of the clan's network such as Mullah Tajmir Jawad, Afghanistan's new deputy intelligence chief. Before being appointed, Jawad allegedly ran a suicide bombing network that orchestrated some of the most lethal attacks in Afghanistan of the past two decades.

Doubts about the Taliban's ability and willingness to live up to its promises are fed even more by the composition of the group's caretaker government, which includes multiple figures designated by the UN and/or the U.S. as terrorists.

Similarly, Mawlawi Zubair Mutmaeen, who once ran Taliban suicide bombing squads in Kabul that struck the presidential palace, a CIA office, and the Kabul Serena hotel, is now a police chief in one of the Afghan capital's districts. To Mutmaeen it is all the same: mediating marital disputes, helping debtors recover their funds, and assisting applicants find jobs as opposed to gathering intelligence, finding weak spots in targets, ordering suicide bombings, and operating a web of informers inside the previous government. "Previously I was serving Islam, and now I'm also serving Islam. There is no difference," Mutmaeen said.

"Until last month he was running a suicide bombers' training camp—that's how favorable an environment [Afghanistan] has become [for Al-Qaeda]. The kind of people that Al-Qaeda treats as their peers or supporters are now moving straight out of the suicide-bomber training camps into running the intelligence service," said Michael Semple, a Dari-speaking former United Nations advisor on Afghanistan and EU representative in the country. He was referring to Jawad but could just as well have been Mutmaeen:

> If you are a member of Al-Qaeda trying to make arrangements to keep your leaders and key operatives safe and out of view and avoiding trouble from the local authorities, what more could you dream of than to have your well-wishers take over the Interior Ministry?

American national security officials fear that perceived Taliban reluctance or inability to control

militant groups means that it is only a matter of time before the IS and Al Qaeda will be able to relaunch attacks in the West. U.S. Undersecretary of Defense Colin Kahl recently told the Senate Armed Services Committee that the IS would regroup in the next six to 12 months while it could take up to two years for Al Qaeda to follow suit.

The doubts are further informed by the Taliban's adoption of a governance model built on an alliance between the state and the clergy that has been part of the Muslim world's problem rather than the solution to its multiple troubles for centuries. As a result, the Taliban's vision of what an Islamic state should look like as well as its emerging attitude since its takeover of Afghanistan towards human, women's, and minority rights as well as and freedom of the press adds to questions about how reliable a counterterrorism partner the group may be.

Pakistani Prime Minister Imran Khan wrote in a *Washington Post* oped that he is

> convinced the right thing for the world now is to engage with the new Afghan government to ensure peace and stability. The international community will want to see the inclusion of major ethnic groups in government, respect for the rights of all Afghans and commitments that Afghan soil shall never again be used for terrorism against any country […]. Taliban leaders will have greater reason and ability to stick to their promises if they are assured of the consistent humanitarian and developmental assistance, they need to run the government effectively. Providing such incentives will also give the outside world additional leverage to continue persuading the Taliban to honor its commitments.

Khan's oped was published three days after 22 Republican senators introduced a bill that, if approved, would mandate the U.S. government to investigate Pakistan's support for the Taliban, as a precursor to the imposition of sanctions. The oped came days before the country's Finance Minister Shaukat Tareen was scheduled to meet in Washington for a review by the International Monetary Fund (IMF) of Pakistan's lending program. Khan didn't help Pakistan by earlier celebrating the Taliban victory as "breaking the chains of slavery."

These doubts and questions go to the heart of a debate about how to coax the group against the backdrop of diminishing Chinese, Russian, Iranian, and Qatari hopes that the Taliban may prove themselves more compromising on the back of their recent victory. China, Russia, Turkey, Iran, Pakistan, and Qatar favor lifting sanctions and maintaining relations even if they are not about to unconditionally recognize the Taliban government. Conversely, the United States and the EU have opted for a more coercive approach, involving sanctions and international isolation. Saudi Arabia and the UAE are hedging their bets, taking their lead from Washington.

Part of the hope that the Taliban may ultimately be more malleable is rooted in the fact that the group is increasingly populated by a generation that came of age during the American-led occupation but has yet to make its mark. Reflecting on the issue, Afghan journalist Fazelminallah Qazizai said:

> Routinely portrayed as archaic and extreme by critics and opponents, the new generation of Taliban are in fact a product of their times: more open to the prospect of gradual social change than their forebears yet politically more militant; English-speaking but mistrustful of the West; well-read yet wary of free expression; keen to help their country move forward but defined by its past.

The Taliban's Quagmire

The Taliban's quagmire was evident when Qatari foreign minister Sheikh Mohammed Abdulrahman Al-Thani described in late September 2021 the Taliban's repressive policies towards women and brutal administration of justice as "very disappointing" and taking Afghanistan "a step backwards." The minister warned that the Taliban risked misusing Sharia law:

> We have […] been trying to demonstrate for the Taliban how Muslim countries can conduct their laws, how they can deal with the women's issues […]. One of the examples is the State of Qatar, which is a Muslim country; our system is an Islamic system [but] we have women outnumbering men in workforces, in government, and in higher education.

"And not only in Qatar. You have Malaysia, you have Indonesia, you have actually all the other Muslim majority countries. [The Taliban] will be just the odd example," added Assistant Foreign Minister Lolwah Rashid al-Khater, the Qatari ministry's spokeswoman. "What we're trying to say is that we're coming from within. We come from within Islam itself. […] We're trying to push through other tracks, like Muslim scholars or imams, to go and speak to them independently from us, from any other government. We encourage them to do that."

The Qatari foreign ministry's effort to position itself as a model of Islamic governance was not only a bid to offer the Taliban an alternative but also an attempt to garner brownie points in a competition with Saudi Arabia and the United Arab Emirates for religious soft power in the Muslim world and international recognition as an icon of an autocratic, yet 'moderate' interpretation of Islam. Hoping for Taliban moderation may, however, be wishful thinking. "Policies are pitched at the group's lowest common denominator to preserve concord. That makes it difficult for the Taliban to change," as *The Economist* noted in October 2021.

Al-Khater suggested that the failure of the international community to lay out a roadmap for the Taliban was part of the problem. As he stated:

> What is it that we're asking from the Taliban? I know that many of us, including ourselves, we put out statements, general statements about women's education, about inclusive government, but is there a piece of paper that is endorsed by the international community that says, "This is what we expect from you. This is roughly the timeline, and this is what you're getting in return?" This has not happened yet, and it's adding complexity over the complicated situation.

As a result, Afghanistan has become the latest arena where religious soft power meets defense, security, and counterterrorism policy. The complexity of that space was evident in the balancing act that Saudi Arabia performed as it sought to distance Islam as practiced in the Kingdom from the Taliban's interpretation of the faith.

Against the backdrop of the rivalry over the ability to project religious soft power, the stakes in Afghanistan are highest for Saudi Arabia and the UAE. Both wishing to clearly distance themselves from the Taliban, the UAE competes with Qatar in having made significant progress on women's rights, while Saudi Arabia has substantially enhanced women's professional and social opportunities since the rise of Crown Prince Mohammed bin Salman. Yet, alongside Pakistan, Saudi Arabia and the UAE were the only countries to recognize the first Taliban government in 1996. Saudi Arabia, moreover, created the Taliban cradle by funding and arming the mujahedeen, helping accelerate the 1980s Soviet withdrawal from Afghanistan.

Former Saudi intelligence chief Prince Turki al-Faisal recently distinguished Wahhabism, the kingdom's ultra-conservative strand of Islam, and Deobandism—another ultra-conservative interpretation of the faith that originated in India—which constitutes the theological wellspring of the Taliban.

Media reports suggested that Prince Turki secretly met Taliban leaders in August 2021. He unsuccessfully sought to convince the group to moderate its policies and put flesh on the notion of a changed Taliban 2.0. As head of Saudi intelligence from 1979 to 2001, Prince Turki dealt with the mujahedeen during the Soviet invasion of Afghanistan and sought to persuade the Taliban to hand over Osama bin Laden after Al-Qaeda bombed American embassies in Kenya and Tanzania in 1998.

The need to distance Islam as practiced in conservative Gulf states from the Taliban interpretation of the faith takes on added significance amid doubts about America's reliability, reinforced by its withdrawal from Afghanistan. It is where religious soft power meets defense and security policy in a court of public opinion that may not delve into the nuanced differences between Wahhabism and Deobandism.

TESTING TALIBAN COMMITMENTS

The Taliban willingness and ability to control militants on Afghan soil may be put to the test sooner than expected. It's only a matter of time before China knocks on Haqqani's door demanding the extradition of Uyghur fighters.

The need to distance Islam as practiced in conservative Gulf states from the Taliban interpretation of the faith takes on added significance amid doubts about America's reliability, reinforced by its withdrawal from Afghanistan.

The Taliban, in a potential bid to preempt a Chinese demand for extradition, have reportedly moved Uyghur fighters out of Badakhshan, the Afghan area that shares a 76-kilometre border with China. The Uyghurs were relocated to Nangarhar in eastern Afghanistan. The relocation constituted a copycat of what the Taliban did when they were in power before 2001. They were replaced by ethnic Tajik fighters, like their brethren on the problematic borders between Afghanistan and Tajikistan, armed with recently captured American-made equipment. The maneuvers belie earlier Taliban claims that all Uyghur fighters had left Afghanistan.

The replacement appeared to be part of a much larger fortification of the Tajik border involving the dispatch of thousands of fighters to Badakhshan and the neighboring province of Takhar that borders on Tajikistan to counter what the Taliban called "possible threats."

At the same time, China appeared to be stepping up its drone surveillance activity using an undeclared forward base in Badakshan that has been manned by Chinese and Tajik forces and no Afghan contingent since the Taliban took Kabul in mid-August 2021. Tajikistan has since offered full control of the bases in exchange for military aid. It also authorized the construction of a second Chinese base on the Tajik side of the Afghan border.

A Chinese demand for extradition would be challenging not only because of the Taliban's consistent rejection of requests for the expulsion of militants that have helped them in their battles. The Taliban already made that clear two decades ago when they accepted the risk of a U.S. invasion of Afghanistan in the wake of 9/11 by repeatedly refusing to hand over Osama bin Laden. There is little in Taliban 2.0 that suggests that this has changed. If Haneef Atamar,

the foreign minister in the U.S.-backed Afghan government of former president Ashraf Ghani, is to be believed, Uyghurs, including one-time fighters in Syria, contributed significantly to the Taliban's most recent battlefield successes in northern Afghanistan.

A demand to extradite Uyghurs to China would also be challenging because Haqqani himself is a wanted man, with a $5 million U.S. bounty on his head. Moreover, the United Nations has sanctioned Haqqani's prime minister, Mullah Hasan Akhund, and various other members of the caretaker government. "It's hard to see a wanted man turning over someone who is wanted for similar reasons," said a Western diplomat.

China appeared to be stepping up its drone surveillance activity using an undeclared forward base in Badakshan that has been manned by Chinese and Tajik forces and no Afghan contingent since the Taliban took Kabul in mid-August 2021.

Likewise, honoring extradition requests could threaten unity within the Taliban ranks. "Taliban actions against foreign jihadist groups to appease neighboring countries would be especially controversial because there is quite a widespread sense of solidarity and comradeship with those who fought alongside the Taliban for so long," said Afghanistan scholar Antonio Giustozzi.

Unanswered is the question of whether and why China would go along with an unspoken international consensus not to seek extraditions if the Taliban keep their word about not striking targets beyond Afghanistan. Assertions that 35 Uyghur militants escaped Afghan prisons during the chaos of the Afghan takeover are likely to call into question any confidence China may have had in the Taliban ability to police foreign militants.

Counterterrorism experts and diplomats, moreover, argue that if forced, the Taliban would quietly let foreign militants leave their country rather than hand them over. That would make it difficult to monitor these individuals. Haqqani's interior ministry announced in early October 2021 that it has begun issuing Afghan passports, prompting concern that militants would be among the beneficiaries.

China has in recent years successfully demanded the extradition of its Turkish Muslim citizens from countries like Egypt, Malaysia, and Thailand and has pressured many more to do so, despite them not being suspected of participation in the Turkestan Islamic Party (TIP). The UN Security Council had designated TIP's predecessor, the East Turkestan Islamic Movement, as a terrorist organization. There is little reason to assume that China would make Afghanistan—a refuge from Syria for Uyghur fighters—the exception.

Chinese foreign minister Wang Yi made that clear when he hinted at possible extradition requests during July 2021 talks with Mullah Abdul Ghani Baradar, a co-founder of the Taliban and the new government's first deputy prime minister. Wang demanded that the Taliban break relations with all militant groups and take resolute action against the TIP. While the TIP may constitute China's major concern, it also worries that China could be targeted in other countries in South and Central Asia by groups like Tehrik-i-Taliban Pakistan (TTP), more commonly known as the Pakistani Taliban.

Already, China is signaling, as is Russia, that it has very few illusions about the Taliban.

The Taliban have probably destroyed any image of reliability in the eyes of the Chinese by demonstrating early on that they speak a different language than the international community, even when they use the same words. The Taliban made clear that their definition of inclusivity was very different than that of other international stakeholders. The Taliban formed an overwhelmingly ethnic, all-male government that was anything but inclusive by the universally agreed meaning of the word. Adding fuel to the fire, Haqqani and his colleagues, including the new military chief of staff Qari Fasihuddin Badakhshani—a Tajik and one of only three non-Pashtuns in the new 33-member government structure—is believed to have close ties to Uyghur, Pakistani, and militants from other countries.

DISAPPOINTMENT GALORE

Already, China is signaling, as is Russia, that it has very few illusions about the Taliban. Russia has twice held military exercises in different formats near Afghanistan's borders with its Central Asian neighbors since the Taliban takeover in August 2021. A bilateral exercise with Tajikistan and, more recently, by the Russian-led Collective Security Treaty Organization (CSTO), were designed to caution the Taliban and reinforce Russia's security role in the region.

Contradictory statements by the Taliban and members of the ousted government of President Ashraf Ghani about whether members of the TIP were in Afghanistan "confirms largely Chinese-Taliban relations really as not very warm," said Niva Yau Tsz Yan, an expert on China's relations with Central Asian nations. "Despite China's various strategies to kind of build this friendship with the Taliban over the last ten years, it hasn't worked."

China's more skeptical attitude was evident when it dropped its reference to Islam in calls for a new Afghan government to pursue stable and productive economic policies only a day after the Taliban took Kabul. China has also subtly suggested that Afghanistan's mineral riches, including copper, lithium, and rare earths such as cerium, lanthanum, and neodymium, may be less attractive than meets the eye at first glance.

China scholars Matthew P. Funaiole and Brian Hart noted that China has learnt the risks of doing business in Afghanistan the hard way. In 2007, two state-owned companies, Jiangxi Copper and China Metallurgical Group Corporation (MCC), signed a $2.8 billion deal for a 30-year lease to mine copper at Mes Aynak. The companies reportedly spent $371 million toward developing the area before putting it on hold amid allegations of corruption and concerns that countless artefacts and ancient Buddhist and Zoroastrian structures could be destroyed. In the same vein, China National Petroleum Corporation (CNPC) signed a 25-year deal to develop an oil field in Amu Darya. Production started in 2012 but was halted a year later.

Analysts read China's insistence on the Taliban maintaining good relations with all its neighbors as an effort to position Central Asian nations as a counterweight to the baggage that comes with ties to Pakistan and Iran.

Similarly, Afghanistan's rare earths are 'light' and more easily found elsewhere, including in China, which is believed to have 37 percent of global reserves that are economically viable and more easily accessible for extraction, including the world's single largest reserve in Inner Mongolia. Likewise, China's efforts to meet its demand for lithium are focused on Latin America's 'Lithium Triangle,' home to 53 percent of the world's economically viable reserves, rather than Afghanistan, which is closer to what was once described by the Pentagon as the potential "Saudi Arabia of lithium."

By the same token, Taliban hopes of benefitting from China's infrastructure, telecommunications, and energy-driven Belt and Road Initiative (BRI) are unlikely to be fulfilled. China and Afghanistan agreed in 2016 to cooperate on BRI. Afghanistan was a year later included in the initiative as part of the $45 billion China Pakistan Economic Corridor (CPEC), China's single largest BRI investment. Yet China never extended that investment into Afghanistan. The nearest China came to looking at infrastructure in Afghanistan were studies on the potential joint development of railroads.

Analysts read China's insistence on the Taliban maintaining good relations with all its neighbors as an effort to position Central Asian nations as a counterweight to the baggage that comes with ties to Pakistan and Iran. China worries that Taliban discrimination and persecution of Hazara Shiites, who account for 20 percent of the Afghan population, could persuade the Islamic Republic to covertly support resistance to the group's rule.

China is also concerned that the Taliban will be reticent about entertaining Chinese-backed Pakistani requests for the handover of members of the TTP. The TTP last year joined forces with several other militant Pakistani groups, including Lashkar-e-Jhangvi, a violently anti-Shiite Sunni Muslim supremacist organization. The Shehryar Mehsud Group rejoined the TTP in October 2021, pledging allegiance to Mufti Noor Wali Mehsud, the TTP's emir.

China fears that the fallout of the Taliban's sweep across Afghanistan could affect China beyond Afghanistan's borders, perhaps no more so than in Pakistan, a major focus of the People's Republic's largest BRI-related investment. The killing of nine Chinese nationals in a July 2021 attack on a bus transporting Chinese workers to the construction site of a dam in the northern mountains of Pakistan raised the specter of Afghanistan-based religious militants jihadists targeting China. Until now, it was mainly Baloch nationalists that targeted the Chinese in Pakistan.

China fears that the fallout of the Taliban's sweep across Afghanistan could affect China beyond Afghanistan's borders, perhaps no more so than in Pakistan, a major focus of the People's Republic's largest BRI-related investment.

EYEING PAKISTAN

The attack occurred amid fears that the Taliban victory would bolster ultra-conservative religious sentiment in Pakistan where many celebrated the group's success in the hope that it would boost chances for austere religious rule in the world's second-most populous Muslim-majority state. "Our jihadis will be emboldened. They will say that 'if America can be beaten, what is the Pakistan army to stand in our way?'" said a senior Pakistani official.

Scholar Muhammad Amir Rana suggested that it may not just be jihadis who are emboldened. "Pakistan's religious landscape is fertile for radical ideologies. As the moderates struggle to make themselves relevant in society, the clergy declares them 'innovators' or *biddati*, who, they say, reject the traditional tenets of the religion," Rana argued.

> The clergy in Pakistan is largely literalist in its understanding of religion and takes pride in being the so-called custodian of tradition. A literalist mind sees the world through very narrow lenses […]. Such a mindset is not healthy for the legal, jurisprudential, and academic discourse of religion, more worryingly when it becomes a political stakeholder it tends to absorb radical tendencies easily.

Indicating concern in Beijing, China has delayed the signing of a framework agreement on industrial cooperation that would have accelerated the implementation of projects that are part of CPEC, a crown jewel of BRI.

Taliban spokesman Zabihullah Mujahid recently kept the Taliban's relationship with the TTP ambiguous, a move seen as de facto rejection of Pakistani extradition requests. "The issue of the TTP is one that Pakistan will have to deal with, not Afghanistan. It is up to Pakistan, and Pakistani Islamic scholars and religious figures, not the Taliban, to decide on the legitimacy or illegitimacy of their war and to formulate a strategy in response," Mujahid said during an interview on a Pakistani television program. The spokesman stopped short of saying the Taliban would abide by a decision of the scholars. Afghan sources suggest that the Taliban advised the TTP to restrict their fight to Pakistani soil and have offered to negotiate an amnesty and the return of the Pakistani militants with the Pakistani government.

The TTP is a coalition of Pashtun Islamist groups with close ties to the Afghan Taliban that last year joined forces with several other militant Pakistani groups, including Lashkar-e-Jhangvi. Intelligence sources estimate that it has up to 5,000 fighters in Afghanistan.

"Our fight against Pakistan will continue until we establish it as an Islamic state. We will not spare their dollar-dependent soldiers and politicians," said TTP commander Molvi Faqeer Mohamad. A wanted man in Pakistan, Mohamad was speaking to Al Jazeera after having been freed from jail in one of the Taliban's many prison breaks. The U.S.-backed government of Ashraf Ghani had refused to extradite Mohamad to Pakistan. Rejecting a Pakistani government offer to grant TTP members amnesty and negotiate, the group's spokesman Muhammad Khurasani insisted "amnesty is generally offered to those who commit crimes, but we are quite proud of our struggle. We can pardon the Pakistani government if it pledges to implement Sharia rule in the country."

Increasingly, the TTP is framing its struggle as a nationalist Pashtun rather than a jihadist quest. "We will free our land from the occupation of the Pakistani forces and we will never surrender to their atrocious rule. We want to live on our land according to Islamic laws and tribal traditions. We are Muslims and Pashtuns," said TTP leader Nur Wali Mehsud in March 2021. In separate remarks three months later, Mehsud insisted that "the independence of Pakhtunkhwa and the Pashtun tribal areas is national and religious for all Pashtuns." Pakistan catered to Pashtun identity when it renamed the North-West Frontier Province as Khyber Pakhtunkhwa in 2010. The region straddles the 2,600 kilometer-border, named the Durand Line by the British, which has never been recognized by Afghanistan.

A few analysts have pointed to what would constitute the greatest threat to Pakistan: the potential coalescing of a campaign of TTP violence with the notion of merging Pashtun-populated areas of Pakistan with Afghanistan. The intertwining of Pashtun national identity and Islam resounds in a Pashto poem quoted by Anas Haqqani, a senior Taliban official and brother of Sirajuddin Haqqani: "The essence of my Pashto is so Islamic. Were there no Islam, I would still be a Muslim." Haqqani quoted the couplet while discussing Pashtun identity with no reference to geopolitics.

Former UK ambassador to Pakistan Tim Willasey-Wilsey predicted that

> Pashtuns of the Afghan Taliban will, after a few years in power, find common cause with their Pashtun kinsmen in Pakistan. […] There are plenty of Pakistani Pashtuns who would prefer the whole of Khyber Pakhtunkhwa [i.e., the former North-West Frontier Province] to be part of a wider Pashtunistan.

Afghans in the Pashtun-majority south of Afghanistan, the Taliban's cradle, have welcomed the security and semblance of law and order that the group's victory has brought about. It was that service provision that first propelled the Taliban in the 1990s to be a force to be reckoned with, in line with Israeli Golani Brigade soldier-turned-economics professor Eli Berman's thesis that the world's most sustainable militant groups trace their roots to service provision. "If we civilians hadn't given them bread, the Taliban wouldn't have won the war," said Mohammad Daoud, a resident of Mua Qala, a town in Helman Province.

Some analysts have privately argued that a Pakistan-dominated Pashtunistan embedded in a broader Asian confederation would counter the various threats Pakistan is concerned about, including the TTP, ultra-conservatism, and secession. The views of these analysts embody the Pakistani military and government's worst fears: the undermining of Islam as Pakistan's glue by ethnic cleavages. It is a fear that was first expressed by Mohammad Ali Jinnah, the country's founder, who warned against the "poison of provincialism." The fear was reinforced by the secession of predominantly Bengal East Pakistan to form Bangladesh in 1971.

"The time is now ripe for America and its allies to marginalize the remnants of radical Islamdom in South-Central Asia as a first step in generating a mega-confederation of free peoples extending from Pashtunistan in the West all the way to and including Indonesia in the East," said a former Western government official-turned-scholar.

> The key step for Pakistan in countering the extremism of radical Muslims trained by the Saudi Wahhabis is simply to absorb the western half of Pashtunistan, which includes the southern two-thirds of Afghanistan, and the eastern half which makes up most of the western third of Pakistan, into a new Province of Pashtunistan in a greater Pakistan confederation as a model for the world and especially for the looser confederation extending across India to Indonesia.)

In 2020, Pakistan cracked down on the Pashtun Tahafuz (Protection) Movement, or PTM, a non-violent protest movement demanding rights for Pashtuns in Pakistan's former Federally Administered Tribal Areas. Pakistan is completing a physical barrier to any changes along the Durand Line that separates it from Afghanistan, with the construction of a $500 million wall.

The wall, conceived to keep militants and potential refugees on the Afghan side of the border, is being bolstered by state-of-the-art surveillance technology and multiple fortresses. Pakistan closed 75 of its 78 border crossings in the wake of the Taliban takeover. Much of the border is mountainous and, in the words of a former Pakistani military officer, "good territory for guerrillas to operate and hide in."

The notion of Pashtunistan or a confederation that includes archrivals Pakistan and India as well as countries as diverse as Indonesia may be far-fetched, to say the least, but is certain to ring alarm bells in Islamabad. Those bells rang louder after Taliban official Sher Mohammed Abbas Stanekzai declared in a rare statement on foreign policy that "we give due importance to our political, economic, and trade ties with India and we want these ties to continue. We are looking forward to working with India in this regard."

Concern about a Pashtun nationalism that could threaten Pakistan's territorial integrity underwrites criticism of Prime Minister Khan's description of the Pakistani Taliban as an expression of Pashtun nationalism rather than religious ideology. "This argument is dangerously flawed. The TTP is a terror outfit that fuels its narrative with religious aspirations instead of nationalistic ones. […] The TTP's acts of terror should not be framed in a manner that may accord it an ounce of legitimacy, especially at a time when it has yet again unleashed violence"—to quote from a recent editorial in *Dawn*, Pakistan's foremost English-language newspaper.

Critics charge caution against reading too much into the predominance of ethnic Pashtuns among the Taliban. Linking "the Taliban, Pashtun nationalism, and religious fanaticism […] represents a gross falsification of the lived Afghan socio-political realities at worst, and an inability to grasp the same at best. Undeniably the Taliban's core leadership is made of Pashtuns; however, to translate that into the Taliban by default representing Pashtun social, cultural, and political ethos is empirically flawed," said international affairs scholar Bilquees Daud. Daud argued that the Taliban have rejected two tenants of Pashtun nationalism:

> Pashtunwali, the Pashtun's secular tribal code that predates Islam, and the notion of a jirga, a council, which arrives at decisions by consensus and has no head. The Taliban declared the jirga system to be un-Islamic a quarter of a century ago.

The notion of Pashtunistan or a confederation that includes archrivals Pakistan and India as well as countries as diverse as Indonesia may be far-fetched, to say the least, but is certain to ring alarm bells in Islamabad.

Nonetheless, scholar and author Pervez Hoodbhoy implicitly appeared to suggest that in some ways the train may have already left the station. "Like it or not, AfPak has become reality. Despised in Pakistan because of its American origin, this term rings true. Geographical proximity is now augmented by the ideological proximity of rulers in both countries. Taliban-style thinking is bound to spread through the length and breadth of Pakistan," Hoodbhoy said. AfPak was a term used by the U.S. government to signal that Afghanistan and Pakistan constituted a single theater of operations in the War on Terror.

Pessimists suggest that may already be happening. Jamia Hafsa, the girls madrassa associated with Islamabad's notorious Red Mosque, has recently flown the Taliban flag from its roof on several occasions while Maulana Abdul Aziz, the radical cleric associated with the mosque, was photographed carrying a weapon. The mosque and its madrassa were raided in 2007 by the Pakistani security forces. At least 100 people were killed in a week-long stand-off with militants inside the compound.

"The coming of the Taliban was an act of God," Abdul Aziz said. "The whole world has seen that they defeated America and its arrogant power. It will definitely have a positive effect on our struggle to establish Islamic rule in Pakistan, but our success is in the hands of God."

SHOWING THEM A FIST

Recent attacks on Pakistani military personnel by the TTP notwithstanding, neither the Taliban nor

Al-Qaeda are believed to want to risk a repeat of actions that prompted the 2011 U.S. invasion. "Al-Qaeda would not like to waste the Taliban's victory again but might like to use their presence in the country to strengthen their regional affiliates in the subcontinent, Yemen, Somalia, and the Sahel," said Abdul Basit, a research fellow at the S. Rajaratnam School of International Studies in Singapore.

Politically, the Taliban are nationalists who want to integrate their Afghan emirate into the community of nations. Unlike Al-Qaeda, the Taliban do not seek to dismantle the existing world order.

Similarly, Sir John Sawers, former head of the UK's MI6 intelligence agency, argued that

> the Taliban will want to focus on consolidating its position in the country. They've also got some important relationships they have got to get right, particularly Pakistan, then Iran and China. All are complicated and none are going to be helped if they become the base of international terrorism.

The determination to operate in ways unlikely to spark the wrath of the United States without making an absolute rupture inevitable has created the basis for bridging theological and political differences between the Taliban and Al-Qaeda. Fine points of theology have prompted hardline Salafis, including the IS and at times elements of Al-Qaeda, to question the Taliban's Muslim integrity. Politically, the Taliban are nationalists who want to integrate their Afghan emirate into the community of nations. Unlike Al-Qaeda, the Taliban do not seek to dismantle the existing world order.

China's dilemma in dealing with the Taliban is reinforced by the fact that Russia with Central Asia as a buffer and a military base in Tajikistan feels less urgency in settling the Afghan issue. As a result, Russia rejected a Chinese request that it recognizes the Taliban government and allows China to go second. "China is running out of instruments to engage with the Taliban," said Yau, the China scholar.

Instead, Russia is hedging its bets, as is Iran. Both countries had helped the Taliban as they rolled across the country in the months before the American withdrawal. The two countries provided funding and weapons and helped them cut deals with groups that paved their road to Kabul. It was those deals that made the difference in the final Taliban push for the defeat of American forces. "We did not anticipate the snowball effect caused by the deals that the Taliban commanders struck with local leaders," U.S. Defense Secretary Lloyd Austin told the U.S. Senate.

Russia and Iran were, however, taken aback when the Taliban refused to form a truly inclusive government rather than one that was overwhelmingly Pashtun at the expense of ethnic Tajiks, Uzbeks, and Shiite Hazaras. The prominence in the government of the Haqqani network, with its history of brutality towards Shiites, was particularly galling for Iran. Giustozzi, the Afghanistan scholar, suggested that Iranian concern about the Taliban predates the recent formation of their government and started with the earlier arrival of nationalist Iranian Baluchi fighters of Jaysh ul Adl, a group that has intermittently attacked targets in the Iranian province of Balochistan while operating from Pakistan and with the support of the Haqqani network.

Pakistan is completing a physical barrier to any changes along the Durand Line that separates it from Afghanistan, with the construction of a $500 million wall. The wall, conceived to keep militants and potential refugees on the Afghan side of the border, is being bolstered by state-of-the-art surveillance technology and multiple fortresses.

Russia was displeased with the breakdown in talks on a future government between the Taliban, former president Hamid Karzai, and former chief executive Abdullah Abdullah. Moscow has signaled its dissatisfaction by holding a series of joint war games in recent weeks with troops from Uzbekistan and Tajikistan, the latter of which hosts a Russian military base and openly supports ethnic Tajik opponent of the primarily Pashtun Taliban. The drills, which involved 2,500 troops from the three nations and some 500 military vehicles as well as artillery, were held close to the Afghan border and included Russian planes striking mock militant camps.

"If the logic of the United States is that its military presence might enhance security of Central Asia, the natural response for Moscow is that 'we can take care of it, we have done it for a long period of time,'" said Andrey Kortunov, director-general of the Russian International Affairs Council. General Anatoly Sidorov, commander of the forces involved in the exercise, emphasized that it was deliberately a high-profile undertaking. He pointed out that his troops were "all visible, they are not hiding." Russia's approach, added Daniel Kiselyov, editor of the Central Asia-focused *Fergana*: "You can talk to the Taliban but you also need to show them a fist."

APPRECIATING TURKEY'S AFGHANISTAN POLICY

Merve Seren

THROUGHOUT history, Afghanistan has suffered tremendously due to the strategic competition resulting from various itinerations of the Great Game, which has in turn shaped and been shaped by the political, military, economic, and sociocultural transformations of the country. Yet, ending up as a "traumatized state" was not only a result of the imperial rivalry between the Russians and the British, nor even of the expansionism of Afghanistan's neighbors, but also due to the country's historical propensity towards bloody revolts, coups, and assassinations plots. Since its establishment, for instance, the Afghan flag was changed nearly 30 times, with a similar fate befalling its national anthem. This only goes to show how deeply entrenched political turmoil and societal unrest are in the history of Afghanistan.

Since the establishment of Turkish-Afghan diplomatic relations, Ankara has conducted an active foreign policy towards this conflict-ridden state. In Turkey's early Republican era, the relationship between the two countries was largely shaped by Afghanistan's attempts at modernization. Its reformist king, Amanullah Khan, looked up to Atatürk's Turkey as a role model.

During the Cold War, Turkey sided with the West (by virtue of its membership in NATO and its rapprochement towards what is now known as the European Union) in the context of an unfolding strategic competition between the Eastern and Western blocs.

And then came the post-Cold War era, which dramatically changed the strategic landscape of the regions surrounding

Merve Seren *is an Assistant Professor in Political Science at Ankara Yıldırım Beyazıt University. She previously served as a senior consultant at STM ThinkTech, Turkey's first technology-based think tank, where she was responsible of war gaming as well as conducting research on issues related to defense, security, and intelligence such as air and missile defense systems, UAV technology, cyber threats, and military spending. She is a former Parliamentary Advisor to the Grand National Assembly of Turkey as a Parliamentary Advisor and Researcher in the Security Studies Department of the SETA Foundation for Political, Economic and Social Research. You may follow her on Twitter @MerveSerennn.*

Photo: Guliver Image/Getty Images

"The Turkish legation in Kabul," unsigned and undated photo

Turkey. Still, Ankara could not immediately recalibrate its foreign policy engagement towards Afghanistan: the latter's domestic, regional, and international dynamics were already heavily influenced by the Taliban. The 2001 U.S. invasion of Afghanistan marked a turning point for Turkey, compelling it to adopt an active foreign policy in Afghanistan within the framework of NATO's ISAF and RSM missions. Turkey seized this opportunity to position itself as a 'noncombatant' military actor with rising soft power.

More specifically, once the Justice and Development Party (AKP) came to power in 2002, Turkey began to perceive Afghanistan as its main strategic leverage in gaining more autonomy in international politics. That being said, this new vision of Turkish foreign policy favored a cooperative security approach (at least in the context of Afghanistan) rather than one that relied on military operations, thus placing greater importance on soft power.

These Turkish tools were utilized in support of the goal of achieving political stabilization as well as the economic and social reconstruction of Afghanistan. Throughout the course of this second longest-running mission in NATO's history (KFOR, which continues to operate

under UN Security Council resolution 1244 (1999) and has included a Turkish contingent since the beginning, is technically the longest-running NATO mission in history), Turkey played a critical role in security and state-building missions, also contributing to provisional reconstruction and infrastructure investment. Ankara enhanced its engagement in war-torn Afghanistan by projecting its soft power capacities among various ethno-linguistic and religious groups.

Ankara sees the consequences of the decision by the United States to withdraw from Afghanistan as a window of opportunity to both re-normalize Turkey's relationship with the United States and to recalibrate Ankara's regional power status. Ankara initially believed that Turkey would gain more strategic leverage and improve its international image by contributing to the political process in Afghanistan. But once the announcement of a U.S. withdrawal signaled that the Taliban would play a more important role in Afghanistan, Turkey's initial plan failed, ushering in a new era of Turkish-Afghan relations whose course remains indeterminate in important ways.

Ankara sees the consequences of the decision by the United States to withdraw from Afghanistan as a window of opportunity to both re-normalize Turkey's relationship with the United States and to recalibrate Ankara's regional power status.

This essay seeks to unpack and contextualize Turkey's strategic rationality in Afghanistan by taking into consideration the dynamics of historical continuities, particularly those concerning their national, regional, and international determinants. Without considering historical continuities, it is not possible to make sense of Turkey's strategic position towards Afghanistan—both over the past 20 years and in the time ahead.

Drivers of Failure

Four related historical processes are critically important to understanding the present failure in Afghanistan, and each in one way or another has had an impact on Turkish ambitions and Turkish foreign policy in that country and, in some cases, further afield. The *first* is an overall Western ignorance of the geopolitical context in Afghanistan. The strategic position of Afghanistan in regional and global geopolitical competition is one of its most essential features. The political, economic, security, and social dynamics within Afghanistan have been repeatedly shaped by power struggles among different foreign actors.

In the late nineteenth century, for instance, the power struggle between the Russian and British empires became the dominant external determinant for Afghanistan. While Great Britain sought to prevent Russian geopolitical expansion towards Afghanistan to protect its primary interest in its Indian colony, Russia's main concern was preventing British territorial consolidation in its near abroad. As part of Great Britain's strategic anxiety, Afghanistan's political landscape was constructed and anchored in the practices of British imperialism, later becoming the main strategic reference point for Kabul's foundational political narrative during the establishment of modern Afghanistan.

The continuity of the periods of British, Soviet, and American domination of Afghanistan is a textbook example in understanding the complex nature of a geopolitical triangle whose three points consist of national, regional, and international constrains.

Later, in the context of global geopolitical competition during the Cold War, Afghanistan became a strategic backbone for the Soviet Union in its struggle against the West. Thus, the same basic geopolitical anxiety, which can be defined as an imperial requirement to protect its sphere of influence and is easily traceable back to the nineteenth century, provoked the Soviet Union to invade Afghanistan in 1979. Notwithstanding the fact that the United States became the mastermind and leading sponsor of the mujahideen resistance to the Soviets, geopolitical competition over the country continued to shape Afghanistan's trajectory even the Red Army left the country in the late 1980s. After the 2001 American invasion, yet another phase of geopolitical competition emerged as part of the changing regional security landscape, which provided a greater role for regional actors and local dynamics.

In addition to the historical aspect of geopolitical competition, geo-economic factors have also shaped the fate of Afghanistan, as it sits on the world's second-largest lithium reserves. With natural resource scarcity being a constant, the control over resource-rich territory was one of the main reasons that drove numerous invasions of outside powers throughout history.

The *second* historical process that is critically important to understanding the present failure in Afghanistan is the country's internal complexities, historically determined by the interaction between external and internal developments. The continuity of the periods of British, Soviet, and American domination of Afghanistan is a textbook example in understanding the complex nature of a geopolitical triangle whose three points consist of

national, regional, and international constrains. While the local resistance to the British Empire was the dominant motivation for political and military mobilization in the late nineteenth and early twentieth centuries, the revolt against Great Britain became the main reference point in the fight against the Soviet Union during the 1980s. More importantly, the resistance against the Soviet Union paved the way for the rise of the Taliban as a key actor on the Afghan scene, ultimately leading to the externalization of geopolitics surrounding Afghanistan.

Moreover, the process of transformation of Afghan politics during the first period of Taliban rule in some ways dramatically changed the historical trajectory of geopolitical competition over Afghanistan. After the 2001 American invasion brought an end to the Taliban regime, a new political mobilization began to shape post-invasion Afghanistan. This time, the mobilization against the Soviet Union became the main reference point for ensuing Taliban resistance against the United States and its NATO allies.

There are many reasons behind the failure to rescue Afghanistan from its decades-long state of collapse. However, one must understand that Afghanistan's war fatigue does not only stem from geopolitical rivalries, but mostly from internal frictions. Some examples of the latter include the eternal dream of establishing Pashtunistan, ethnonationalism, and sub-nationalism—that is to say, realities and myths about tribes, sub-tribes, as well as clans and khels. This will be discussed at some length below.

While the initial plan was to overthrow the Taliban regime and eliminate al-Qaeda, the U.S. strategy of counterterrorism was transformed into one of state-building.

The *third* dynamic concerning the failure in Afghanistan relates to America's strategic conception of preemptive war, made most manifest during the presidency of George W. Bush, which neglected conventional determinants. In the post 9/11 era, Afghanistan turned out to be the most important country to the implementation of an American-centric vision of counterterrorism. While the initial plan was to overthrow the Taliban regime and eliminate al-Qaeda, the U.S. strategy of counterterrorism was transformed into one of state-building. NATO's post-2001 mission and the nation-building project ignored and undermined the aforementioned three pillars of Afghanistan's political landscape. This ultimately led to the re-emergence of three existential threats to the future of Afghanistan under the second Taliban rule. Each requires a somewhat lengthy account because the details are largely unknown to most outside observers.

The first existential threat is Afghanistan's territorial integrity, a fragile construct built on artificial borders drawn in 1893 by the British Empire in a treaty that established the Durand Line. This line separates Afghanistan from Pakistan and continues to be a disputed demarcation—a fundamental security issue still waiting to be resolved. Despite having received substantial support from Pakistan since the early 1980s, even the Taliban never formally recognized the Durand Line. Hence, the line appears to remain a fundamental obstacle to managing the volatile Afghanistan-Pakistan relationship. However, the Durand Line is not to be considered a simple territorial issue. It serves an ethnic claim, whose aim is to unite all 'Pashtuns' and establish a state of Pashtunistan. While the Pashtuns constitute the largest segmentary lineage group in Afghanistan, they are the second-largest in Pakistan's ethnic composition, after the Punjabis.

The second existential threat the future of Afghanistan under the second Taliban rule is ethnonationalism, since the Pashtun ethnicity has been directly associated with the state ideology and societal identity. Afghanistan was founded by Ahmad Shah Durrani in 1747 with the unification of various Pashtun tribes. Their nationalism has become the state ideology under the rule of King Mohammed Nadir Shah, who changed Afghanistan's destiny at the beginning of 1930s by amending the constitution in a modernist manner. Indeed, following Nadir's rule, the state's legitimacy has relied on nationalism rather than Islam. Accordingly, citizenship became linked with the feeling of belonging, innately specified to a certain nation, with a common history rewritten to reflect a narrative of a shared ethno-biological basis.

Although there were some attempts to remedy the problem of discriminatory citizenship—like amending the term "Afghan" to depict all citizens rather than being used synonymously with "Pashtun"—Pashtunization remains an unresolved issue. In fact, the United States and its allies have been widely accused of exacerbating the Pashtunization problem in Afghanistan, especially with regards to decisions made in the wake of the 2001 Bonn Conference. This is believed to have been the first step in a Pashtun-centric nation-building project.

Conversely, Turks, Tajiks, and Hazaras voice their objections for being underrepresented as ethnic groups. It is alleged that the percentile distribution to ethnic groups in the country's demographic image has long been fabricated as part of a "Pashtunization project." Interestingly enough, the first and only national census in Afghanistan was conducted just before the 1979 Soviet invasion, which lacked precision (since

then, several surveys were carried out, but none aspired to reach the level of a general census). Still, a lack of confidence in the results has resulted in a failure to make comprehensive, accurate, and reliable analysis of the country's ethnic diversity. Indeed, Afghanistan's multiethnic composition is much wider than is conventionally thought. For instance, 200 different ethnic groups were identified in a study conducted by the Soviet Union and 54 were described in one conducted by Germany. Yet only 14 of them are recognized in Afghanistan's 2004 Constitution.

Nevertheless, ethnicity remains one of the major obstacles to mitigating risks and threats stemming from the demographic transition in Afghanistan. Both Hamid Karzai and Ashraf Ghani were accused of staying silent while the Taliban were steadily expanding their territorial control from the south to north. Especially noteworthy were the Taliban's operational successes in Afghan Turkestan, where significant gains were made without anyone putting up a real fight. In other words, both post-9/11 Afghan presidents stand accused of allowing the Taliban to capture districts of northern Afghanistan to enact a strategy of "forced demographic change," all done as part of a Pashtunization process.

The third existential threat relates to both "tribalism" and "clanship." These are the most complex concepts and phenomena to comprehend, since they exist as "reconstructed" political and social realities of Afghanistan. In addition to ethno-nationalism, preexisting divergences of interests among various ethno-linguistic groups have worsened over time. Tribal rivalries and clan tensions have evolved into a more chaotic power struggle. Decades-long rivalries between Pashtun tribes—mainly the clash of a group of intellectual elites known as "Abdali" or "Durrani" and poor locals termed "Ghilzai"—indicate tribal factionalism among Pashtun nationalists. The tribal game was also present in the political contest between Karzai, who belongs to Durrani, and Ghani, who is of Ghilzai origin, but more famous as a "Kuchi"—a name assigned to Afghan nomads. Relevantly, it is alleged that Ghani deliberately left the capital to the Ghilzai-dominated Haqqani Network, before fleeing the country on 15 August 2021. The Taliban, on the other hand, whose co-founder is Mullah Baradar from the Durrani tribe, had captured other metropolitan areas, such as Kandahar and Herat (and, of course, Kabul).

Although the rivalry between Durrani and Ghilzai Pashtuns has been ongoing for centuries, the latter have succeeded in taking over national power only four times; under Mir Wais in 1721, Nur Mohammad Taraki in 1978, the Taliban under the rule of its first supreme leader Molla Omar in 1996, and again the Taliban in 2021 under its new leader Mawlawi Haibatullah Akhundzada. Therefore, when analyzing the drivers and influences of the Taliban insurgency, one must first understand tribalism and clanship in Afghanistan in order to fully comprehend the nature and character of the Taliban movement.

However, the problem is much more complicated than the well-known conflict between Durrani and Ghilzai tribes. In addition to various tribes (zai), there are also sub-tribes (khel)—and clans and sub-clans, too. The role and significance of tribalism and clanship in Afghanistan can be traced back to 1921, when a special department was established during Amanullah Khan's kingship—an institution that can be regarded as the predecessor to the Ministry of Border and Tribal Affairs. Furthermore, recently issued ID cards (called "Tazkira") indicate the tribal/ethnic backgrounds of Afghans—a rather controversial novelty in light of Ghani's attempt to create an inclusive 'Afghan' category of common nationality for all ethnic groups in the country.

Indeed, 'intra-tribal cohesion' and 'tribal representation' will also be a challenging test case for the Taliban in its second attempt to rule Afghanistan. On the one hand, tribal ties are an important element that bind the core leadership and the commanders—preventing political fragmentations in the organization. On the other hand, nurturing such ties allows the Taliban to continue to engage in an 'inclusiveness discourse'—one of the main criteria to be recognized as a legitimate government and a major step to lift the sanctions and start diplomatic and economic relations with other countries.

The above-mentioned existential threats that were misread and/or underestimated by the U.S. and other coalition forces remain the uppermost drivers of the 'relative peace' that was lost in Afghanistan. Analyzing Taliban fundamentalism within the limits of religious ideology was nothing more than trying to neutralize an octopus by cutting only one of its eight tentacles.

The *fourth* and final historical driver behind the present failure in Afghanistan should be understood in the context of Taliban's strategy of resistance that undermined the post-2001 political transformation in the country. The first dynamic that strengthened the Taliban's political and military mobilization is the severe use of force by the U.S. military in Afghanistan. While the coalition's military strategy was successful in its early stages—succeeding to push back the Taliban and to minimize its territorial control—over time the fight against al-Qaeda caused unpresented civilian casualties. This led to the emergence of a resistance narrative,

which provided a golden opportunity for the remobilization of anti-NATO partisans.

Another vital dynamic that gave more maneuvering space to the Taliban was poor governance in dealing with social, economic, and political issues as well as the lack of effective Security Sector Reform (SSR) in the context of NATO's mission of creating a fully capable Afghan National Defense and Security Forces (ANDSF). More importantly, the strategy of irregular (read: guerilla) warfare against the U.S.-led coalition also played an important in positioning the Taliban as the major security provider for the local population. The territorial gains made during the process of U.S. withdrawal provided more opportunities for the Taliban to ensure local consent and win over local population. This, in turn, accelerated the downfall of the U.S.-sponsored and supported Afghan state apparatus.

Turkish Strategic Reasoning

Against this backdrop, Turkey's Afghanistan policy should be understood with reference to the historical trajectories of Afghanistan. Out of all NATO member states, Turkey has always been the most advantageously-placed to deal with Afghanistan-related issues. Turkey's Afghanistan policy can be divided into two basic temporal periods: the past and the past-present (if it can be put this way). While history is significantly important, it is not the only determinant—Turkey's policies during the NATO mission is also a particularly important indicator of the internalization of the historical dynamics toward Afghanistan.

Out of all NATO member states, Turkey has always been the most advantageously-placed to deal with Afghanistan-related issues.

Afghanistan has always represented a unique place for Turkey, as both an ancestral home of sorts and as a land whose religious and cultural heritage deserves to be protected. Afghanistan has been a Turkic dwelling-place since the second century BC—from the Iskits and Hephthalites to the Ghaznavids and the Seljuqs of the Oghuzs, Khwārezm-Shāh to the Chagatai, the Mongols, the Timurid, and of course the Mughals. The great Turkic ruler Babur Shah's tomb in Kabul and Rûmî's journey from Belkh to Konya are only two examples indicating why Afghanistan is a distinctive destination for Turkic people in particular and many Muslims in general. This historical linkage has been produced and reproduced by many official statements in creating the meta-narrative of Turkish foreign policy.

Although Turkish-Afghan relations trace back to the Ottoman period (precisely, the eighteenth and nineteenth centuries), the relationship has not always been a favorable and beneficial one—as evident from Sultan Abdulhamid's 1877 failure to form an alliance to counter Russian threats. However, this began to change by the early twentieth century, when Afghanistan gained independence from Great Britain through the 1919 Rawalpindi Agreement. Over time, Turkish advisors, doctors, teachers, military officers, and technocrats were sent to Afghanistan. Even during a very critical period—the Turkish War of Independence (1919-1923)—Atatürk assigned numerous delegations to provide medical and law enforcement training to Afghanistan. The arrival of technocrats and experts to Afghanistan also demonstrates that a series of reforms were undertaken in the scope of Afghanistan's first state-building project, drawing on important lessons learned by Turkey's own modernization drive.

In return, Afghans responded to Turkey's calls to join the anti-imperialist struggle with equal sincerity and support. Young Afghans that studied in Turkey at the time and infantry platoons that arrived directly from Afghanistan joined Turkish troops in the Anatolian War. Moreover, many Afghans contributed small donations to Turkey's war effort, despite the country's poverty. While Turkey was still waging a full-scale war for independence, Afghanistan formed and secured its diplomatic relations with Turkey through the Treaty of Alliance, adopted by the Ankara government on 1 March 1921. Afghanistan became the second country (after Armenia) to recognize the Turkish Grand National Assembly. Likewise, the first embassy of the new Turkish state opened in Kabul, which also holds the distinction of being the first diplomatic mission to be inaugurated in an independent Afghanistan. As a remarkable ally, Afghanistan has always offered consistent commitment to support Turkey's survival. For instance, at a dinner served in honor of the Turkish Government on 31 July 1921, the Afghan ambassador openly threatened to declare war on London if it dared wage war against Turkey. He added that if the British were secretly helping the Greeks, Afghanistan would utilize tribes to wreak havoc on the North-West frontier of India.

Consequently, the Turkish-Afghan relationship evolved into a lasting friendship during the Atatürk period. Atatürk's Turkey became both a role model and a key ally for King Amanullah Khan's Afghanistan. Bilateral relations reached at their highest level in 1928, when the monarch paid a visit to Turkey and signed the first Technical Cooperation Agreement between the two countries.

However, Atatürk warned Amanullah to handle the modernization project with care, reminding him to take into

account the differences in values, attitudes, and perceptions between Turkish and Afghan societies. Since Atatürk was highly aware of the difficult circumstances and worst-case scenarios, he advised Amanullah to consider the characteristics of Afghan society as *sui generis*—in other words, to develop a unique modernization model to implement Western-style reforms pertaining to Afghanistan's own dynamics. Atatürk's advice, however, was not heeded. Amanullah's optimistic and perfectionist approach soon resulted in a rapid decline of public support, strong resistance from enraged religious figures, and a chaotic tribal revolt—all of which forced Amanullah to abdicate the throne in January 1929.

Bilateral relations mostly developed and gained momentum during the eras of Amanullah Khan, Nader Shah, and Zâhir Shah. Not only did Ankara make significant investments in Afghan education and infrastructure, but Turkey also played a crucial role in resolving the Afghan-Iranian territorial dispute. Furthermore, Ankara provided huge political support to Kabul in Afghanistan's successful campaign to gain membership in the League of Nations and become a signatory to the 1937 Saadabad Pact (a treaty signed in Tehran involving Afghanistan, Iran, Iraq, and Turkey).

While the Turkey-Afghanistan relationship never experienced a major breakdown, the overall level of this strategic partnership remained quite low and its effects relatively limited. This was mainly due to the frequency of crises and paradigm-shifting events that occupied the attention of both states. Obvious examples that diverted attention away from the bilateral relationship include World War II, the Cold War, numerous coups in both countries and elsewhere, the Soviet invasion of Afghanistan, the Afghan Civil War, and finally, the rise of the Taliban regime.

NATO and Turkish Soft Power

Since the early 2000s, Turkish foreign and security policy towards Afghanistan has been subjected to critical changes. Evidently, 9/11 focused global attention on Afghanistan: the Taliban-led country was labeled a "terrorist safe heaven," and so on. Turkey's security concerns were further triggered by the 2003 Istanbul bombings—a series of mass-casualty suicide attacks carried out by Al-Qaeda. This led Ankara to support landmark anti-terrorism resolutions adopted by the UN Security Council as well as NATO's new counter-terrorism measures.

From the very beginning, Ankara was highly aware that Bush's War on Terror and the U.S-led nation-building project had serious deficiencies, were based on incorrect assumptions, and utilized the wrong tools for Afghanistan. Therefore, Turkey attributed critical importance to

bringing its knowledge and experience to the various international missions present in Afghanistan by engaging in peacebuilding and state-building efforts within ISAF and RSM, and, in particular, capacity-building of ANDSF within SSR.

Turkey undertook the command of ISAF-II (2002-2003); assumed the leadership of ISAF-VII in 2005, the same year it took over the running of Kabul's airport; inaugurated the Turkish Provincial Reconstruction Team in Wardak (near Kabul) in 2006; undertook the command of Regional Command Capital (RC Capital)—which was comprised of Kabul city and 14 districts of Kabul province—between 2009 and 2014 on a rotational basis with France and Italy; established the Gazi Military Training Center to train non-commissioned officers and soldiers in 2010; and started contributing to NATO's new non-combat RSM mission in 2015. Following the Turkish parliament's approval to extend the deployment of troops for 18 more months as part of NATO mission in December 2020, the handover of duties took place in NATO Headquarter TAAC-C in Kabul, between Turkish Brigadier Generals Ahmet Yaşar Dener and Selçuk Yurtsızoğlu, in March 2021.

From the very beginning, Ankara was highly aware that Bush's War on Terror and the U.S-led nation-building project had serious deficiencies, were based on incorrect assumptions, and utilized the wrong tools for Afghanistan.

Being very familiar with the internal dynamics of Afghanistan, Turkey—despite American pressure—consistently refused to play a combat-role in the country, in an effort not to damage the feelings of brotherhood between two nations. In the meantime, apart from security missions, Turkey became one of the leading foreign contributors to Afghanistan's peace, stability, and welfare. Turkey not only trained thousands of Afghan military and police officers, but also made it possible for thousands of Afghan girls and boys to have equal educational opportunities by constructing 21 schools and four educational centers across eight provinces.

Indeed, Turkey's urge to increase its soft power and to deliver on its commitments to invest in a better future for Afghanistan is evident from the activities of many Turkish institutions, including the Turkish Cooperation and Coordination Agency (TIKA), YTB, and the Maarif Foundation. TIKA, for example, successfully completed more than 1,000 projects on education, culture, health, agriculture, and infrastructure through its offices in Kabul, Herat, and Mazar-i-Sharif.

Additionally, the Turkey-Afghanistan Business Council was established in

2002 under the Foreign Economic Relations Board of Turkey (DEİK), which ensured Turkish contractors were able to play a more active role in the reconstruction of Afghanistan. Almost 700 projects were successfully completed by hundreds of Turkish companies operating in Afghanistan, ranking the country first among foreign investors in Afghanistan's construction sector.

While the majority of projects were in the field of contracting and engineering consultancy, Turkish companies also showed an increasing interest in investing in energy and mining. For instance, the Turkish Afghan Mining Company (TAM) was established as a joint venture between Turkey's Yıldızlar Holding and Afghan Gold and Minerals Consortium (led by Afghan entrepreneur and politician Sadat Naderi and a U.S.-based mining and exploration company CENTAR).

In 2018, for example, TAM announced the signing of two contracts with the Afghan government to develop two sites in the Balkhab District in Sar-e Pol and Badakhshan. This represented the largest gold and copper mining exploration effort in the history of Afghanistan. However, in December 2019, the spokesperson of Afghanistan's Ministry of Mines and Petroleum declared that the contracts had been terminated on the grounds that TAM could not fulfill commitments made during the bidding process. Allegedly, the real reason behind the cancellation was the upcoming election in Afghanistan. This example illustrates the deep roots of ethnonationalism in the country (and, of course, how conflict-of-interest rules Afghanistan). Without getting into the details, suffice it to say here that the aforementioned Sadat Naderi is the son of Hazara's famous politician and religious leader, and that his brother Sayed was the security advisor to Abdul Rashid Dostum, the famous ethnic-Uzbek leader who was a member of the Northern Alliance and later served as the country's Vice President during most of Ashraf Ghani's term in office.

Despite its failures, TAM set a good example of how mutual benefits and win-win cooperation could result from the management of natural resources—that is to say, not only to further financial gain for a Turkish company, but also to contribute to changing Afghanistan's internal dynamics—with potentially far-reaching geopolitical implications. The project showed that if Afghanistan could come to manage its natural resources with the help of a trusted ally, then many of the parameters of insecurity and instability—such as economic dependency, drug trafficking, corruption, lack of public services, local conflicts, insurgency, immigration,

public health risks and environmental hazards—might be solved.

STRATEGIC PRIORITIES

Turkey's strategy in Afghanistan is shaped by local, national, regional, and global dynamics. During the process of the U.S. withdrawal, Turkey saw that the Afghanistan issue represented a golden opportunity to re-normalize its relations with the United States. Since the beginning of the Arab Spring, the partnership between the two countries has been on a downward trajectory due to a shift in Washington's preferences, particularly in the Syrian conflict. Under the Obama Administration, the U.S. adopted a strategy of defeating ISIS by supporting the PYD and the YPG, despite both being organic Syrian offshoots of the PKK, which has been listed by the U.S. State Department as a foreign terrorist organization for more than two decades. The Trump Administration maintained the same strategy and preferred to consolidate the YPG's territorial control. So far, the Biden Administration has upheld similarly close cooperation with the PYD and YPG.

While Washington's continued strong support for Syrian both the PYD and the YPG remains the most severe challenge in the bilateral relationship, Turkey's purchase of the Russian S-400 missile system deepened strategic disagreements between these two NATO allies, since the U.S. perceives Russian technology and its technical support as an intelligence threat against the F-35 fighter program. The disagreement concerning Turkey's S-400 procurement led the Trump Administration to impose CAATSA sanctions on Turkey, which basically means Turkey will be unable to purchase this next generation of combat aircraft.

Therefore, in the initial stage of the U.S. withdrawal, both Ankara and Washington thought the Afghanistan situation could come to represent a momentous occasion for the two allies to finally reach a deal on the re-normalization of the bilateral relationship. In this context, given its well-known expertise and experience, Turkey emerged as a key player for continuing to run and maintain the Kabul airport—an obviously fundamental and complex duty, given the volatility of the situation on the ground. However, America's mismanagement of its withdrawal and the Taliban's rapid and complete victory changed the bilateral agreement between the U.S and Turkey.

In the aftermath of the Taliban return to power in 2021 and the establishment of a Taliban-led interim government, Turkey has continued to focus on Afghanistan—not as part of its strategic relations with America, but rather as part of its own foreign and security policies' priorities. Three dynamics are important to understand

Turkey's strategy vis-à-vis Afghanistan under Taliban rule.

The *first dynamic* is shaped by Turkey's domestic concerns regarding migration issues. As the literal geographic bridge connecting East and West, Turkey has always been affected by intense waves of migration from Middle Eastern countries. The migration flux from Syria to Europe in the last decade was especially challenging for Turkey, with a broad range of issues still being managed.

In the aftermath of the Taliban return to power in 2021 and the establishment of a Taliban-led interim government, Turkey has continued to focus on Afghanistan—not as part of its strategic relations with America, but rather as part of its own foreign and security policies' priorities.

The year 2021 was the seventh year in a row marking Turkey as the home to the largest number of refugees in the world; nearly 4 million Syrians are registered as being "under temporary protection" and more than 350,000 others (mostly from Afghanistan, Iraq, and Pakistan) enjoy a similar status. While Syria and Afghanistan continue to be the largest source of migration to Turkey and the region, a new wave of Afghan migrants fleeing the return of the Taliban has pushed Turkey's absorption capacities and resources to the limit, given that the impact of the migration wave from Syria has not subsided yet. Therefore, along with observation towers built along the Turkish-Iranian border, Turkey's control of Kabul Airport—together with Qatar—is also important for managing the migration issue and strengthening Ankara's hand in its relations with Western countries.

The *second dynamic* is shaped by Turkey's local and global security concerns as Afghanistan reemerges as an exporter of radicalism, violent extremism, terrorism, and separatism. Indeed, there are more than 20 terrorist organizations operating in Afghanistan today that can develop tactical and strategic collaborations with or against the Taliban. Primarily, al-Qaeda and the Haqqani Network remain potential threats to the Taliban. The FBI has placed a $10 million bounty on the head of the Taliban government's Interior Minister, Sirajuddin Haqqani. If the Taliban wish to be recognized—more than 15 terrorists hold ministerial portfolios in Afghanistan's current government—it must first conduct 'intra-Taliban negotiations.'

In addition, the Taliban's choices with regards to how it relates to foreign fighters and other terrorist groups like the TTP, ISIS, the ISKP and the PKK will be a key determinant for Turkey's future involvement in Afghanistan. The Taliban's choices will not only show whether it has the political and military power to secure Afghanistan, but also reveal the nature of its objectives and approaches. For instance, a lack of Taliban fighting capability might lead to an increase in ISIS threats or FTF mobilizations towards Turkey. Likewise, the security vacuum and poverty in Afghanistan might increase opium cultivation and production. This could, in turn, increase illicit drug trafficking, which poses a critical threat to Turkey—the country is a key pathway to the route to the EU that passes through the Balkans—as it offers the PKK an intensified cooperation with the Taliban and other organized criminal groups.

The U.S. withdrawal from Afghanistan may lead to the creation of a new "Taliban model" for likeminded movements to emulate—after all, the Taliban can be credibly portrayed as having defeated the United States and its international coalition forces on Afghan soil despite very limited resources.

Above all, the U.S. withdrawal from Afghanistan may lead to the creation of a new "Taliban model" for likeminded movements to emulate—after all, the Taliban can be credibly portrayed as having defeated the United States and its international coalition forces on Afghan soil despite very limited resources. 'Taliban romanticism' might be a reference model for other fundamentalist groups and terrorist organizations that can spread extremism and terrorism in the region.

Finally, the second Taliban era might deepen and widen ethnic and sectarian wars in the region. In fact, the post 9/11 era already revealed that sectarian wars had replaced ethnic ones, leaving open the possibility of witnessing more destructive, lethal, and longer sectarian wars in geographies all over Asia and Africa in the context of the second Taliban era.

The *third dynamic* is shaped by Turkey's urge to play a geopolitical role. Under the AKP's rule, Turkey remains committed to the goal of being a regional power and a more influential global actor, which requires regaining international prestige. Thus, continuing engagement in Afghanistan is important for Turkey's power projection, not only militarily but also in terms of soft power. If another international coalition force is formed in Afghanistan, it will likely be an Eastern one—in contrast to Western involvement of the past two decades. Therefore, Turkey's strategic partnership with Qatar, or a new regional consensus that it may reach with Pakistan, Iran, Russia, China, India, and the neighboring countries such as Uzbekistan, will be very important for the country to consolidate its geopolitical gains.

What's Next?

Turkey will continue to support peace in Afghanistan for the sake of preserving its historical, ethnic, social, and cultural heritage, but also in furtherance of its own geopolitical and geo-economic interests. Potential unrest or outright civil war in Afghanistan would subject Turkey to another unwanted wave of mass migration, raising not only border security concerns but also causing a humanitarian crisis, enabling terrorist flows, and imposing additional financial burdens—issues that could determine the upcoming elections in 2023.

Turkey will continue to support peace in Afghanistan for the sake of preserving its historical, ethnic, social, and cultural heritage, but also in furtherance of its own geopolitical and geo-economic interests.

Apart from its official narrative, which is based on the nostalgy for 'brotherhood,' sustainable peace and development in Afghanistan will benefit Turkey's overall interests the most. Therefore, Turkey's historical responsibility, along with its geopolitical and geoeconomics interests, will shape the country's involvement in Afghanistan.

So far, Turkey has employed a cautious engagement strategy with the Taliban's Afghanistan. Ankara's discourse and attitude has been similar to that of its Western allies: open for dialogue, but not ready for recognition. Although, unlike some Western countries, Turkey has never pursued any sort of "carrot and stick" policy, since Ankara is acutely aware that this could only invoke unwanted traumatic memories in Afghan circles, causing mistrust and ruining relations. Realizing that the Taliban cannot be a controlled with carrots and sticks in the long-term, Ankara appears to believe that the 'gradual engagement criteria' must be flexible and adapted to Afghanistan's internal dynamics.

Clearly, it is vital to comprehend what to expect from the Taliban: a mujahedeen, terrorist political actor that is largely composed of nationalist Pashtun Molla's and Qari's, heavily influenced by both Deobandi and Salafism, and trying to apply Islamic rules in its pure and primitive form. It would be irrational to expect them to embrace a Western-style democracy or even the Western concept of the rule of law and human rights. Their 'ulema' mindset is what it is: Turkey's engagement criteria must be unique and tailored to respond to the Taliban's standards and limits. In return, given Afghanistan's dependency on foreign aid and inflows of money, it seems that the Taliban do not have much of a choice other than to sacrifice its fundamentalist ideology to a certain extent and to present an acceptable level of 'inclusiveness' and 'openness' in order to establish sustainable governance.

Therefore, Turkey's involvement will be shaped by decisions made by the Taliban leadership: either striking a balance between their fundamentalist and tribalist ideas whilst complying with the current world order; or preserving its insurgent mindset and continue to rule as a closed regime. If its leadership selects the first option, then Turkey will be the gatekeeper for the Taliban's engagement with the West. If the Taliban choose the second option, it is highly likely that its monopolist approach will plunge the country back into civil war, which will once again be supported by the West.

Their 'ulema' mindset is what it is: Turkey's engagement criteria must be unique and tailored to respond to the Taliban's standards and limits.

Three Lessons

The United States, NATO, and partnering countries spent 20 years attempting to either survive or leave Afghanistan to the Taliban rule. All the great powers—Great Britain, the Soviet Union, the United States—could not escape the Afghan trap; a heavy political and financial burden caused by lost lives and operational costs. There is no doubt that there are many lessons to be learned from the Afghanistan case, yet three of them bear the biggest significance for the future.

The *first* one is the impact of religion in the country. Western-style policies in countries like Afghanistan might work in the short- and medium term, but these are highly likely to face resistance in the longer-term. Although the Soviet Union or the U.S. intervened upon the invitation or permission of the Afghan state, after a while they were both labeled as 'occupying powers.' While the American endeavors to create a democratic country were highly appreciated by some stratum of people living in Kabul and nearby cities, in the more conservative southern and eastern provinces these ignited fear and anger, which were followed inevitably by attempts to preserve their religious identities and socio-cultural structures. For these reasons, the Taliban successfully imposed their own form of justice by establishing 'shadow governance' in the rural areas. For example, the self-proclaimed judges sitting in Taliban tribunals kept delivering sentences such as stoning, flogging, and amputation.

The *second* lesson is the significance of socio-cultural intelligence in analyzing internal dynamics—especially the local actors and conditions in Afghanistan. For 20 years, many of the Western countries based their assessments on information collected from Kabul or other cities, which led them to misread

trends in Afghanistan as a whole. Socio-cultural intelligence requires the ability to gain deep insight: 'mirror imaging' tends to be easier for people who share the same religion and have similar enough social and cultural values. This explains why so many Western analysts claimed that Ghani's flee, the Taliban's territorial expansion, and Kabul's fall were "surprising" and "shocking." However, on the ground the picture could not have been clearer: the "Pashtunization project" was gaining momentum and the rivalry between the Durrani and Ghilzai tribes was becoming more evident in the last decade. The fact that the Taliban displaced non-Pashtun ethnic groups from captured regions—e.g., Daykundi and Panchshir—and replaced them with Pashtuns is a concrete example whose significance, at least, went largely unnoticed in all too many Western circles.

The *third* lesson has to do with the failure of 'exporting' leaders to other countries. Hamid Karzai, Ashraf Ghani, Zalmay Khalilzad, and Şir Mohammad Abbas Stanikza were all radical Pashtuns who were given support to bring peace for Afghanistan. It must always be kept in mind that the fate of Afghanistan should be determined by the Afghan people. In a similar manner, a strategy of eliminating one terrorist group by creating another cannot succeed in the long run. Thus, supporting ISIS or ISIS-K, or transforming "resistance groups" into "proxies" will not work for Afghanistan. Forcing people to choose with some version of the famous post-9/11 phrase "either you are with us, or you are with the terrorists," will only pave the way for new insurgencies and civil wars in the future.

THE RISE AND FALL OF TURKISH FOREIGN POLICY

Süha Umar

WHEN my esteemed friend Vuk Jeremić, Editor-in-Chief of *Horizons*—a journal I follow closely and from whose articles by distinguished contributors I have benefited from the very first issue—asked me to write an essay on the foreign policy of Turkey, I immediately thought that it would be very easy. It would contain only one short sentence: "Turkey has had no considered foreign policy since 2002, when the Justice and Development Party (AKP) first came to power." What follows is an elaboration on this one sentence—an explanation of sorts for those who might wonder what the above sentence is really about. My essay ends with an earnest challenge to those who might disagree.

THE RISE

After 44 years, including 15 years as ambassador who actively served at the Ministry of Foreign Affairs of Turkey until 2011, I was sure that I had come to grips with at least the basic principles of the foreign policy of the country I was representing. Some of these principles were: peace at home, peace in the world; non-interference in other countries' internal affairs; seeking regional and worldwide cooperation, if and when possible, through regional and global pacts and organizations to advance peace and stability.

These and some other guidelines I will have occasion to discuss in what follows had always been kept in mind by those who conducted Turkish foreign policy since the Republic of Turkey was founded by Mustafa Kemal Atatürk and the Grand National Assembly in 1923, following the War of Independence.

The "National Struggle" (Milli Mücadele), as it is known to us Turks, was a unique war that represented a fresh start for Turkey—one that had risen from the ashes of an empire when the victorious Allied Powers of World War I brought to an end to the Ottoman period of our history. During this period, lest we forget, the UK had attempted to take over control of the Turkish Straits, the main bone of contention between the British and Russian empires for several centuries. France, Italy, and Greece, for their part, had tried to take hold of parts of Anatolia and Thrace. We should also not forget that the Armenians and the Kurds, with the encouragement and support of the Allied Powers, each also expected to be able to carve out a state for themselves, most of the time claiming the same territory in the east and southeast of Anatolia. All this went against the new republic's commitment, made at the very onset of its existence, what imperative to keep as its homeland, declaring this in a "National Pact" (Misak-ı Milli) adopted by the Grand National Assembly. In this way, the state made a public commitment that it would not opt for irredentism but would also not give up what was its own.

Empires die hard and very slowly: such a death leads to many recriminations and claims that might not disappear for centuries.

One last word on the main pillars of the Turkish foreign policy: the War of Independence was the first uprising in the world against imperialism, and, as a result of this, the foreign policy of the Republic of Turkey was founded on anti-imperialism, too.

A few words on the republic's political system are also in order. The Turkish political regime had opted for true democracy even during the years of the War of Independence, with Mustafa Kemal Atatürk always working with the Grand National Assembly, the members of which were freely chosen by the people. The 1921 Constitution declared that sovereignty belonged unconditionally and with no restrictions to the nation, and the 1923 revision made it clear that Turkey was a republic. The Constitution as revised again or rewritten in 1924, 1928, 1937, 1961, 1982, and so on further stipulated that the Republic of Turkey was a democratic, secular, and social state, governed by the rule of law.

Empires die hard and very slowly: such a death leads to many recriminations and claims that might not disappear for centuries. To this we can add that the Ottoman Empire was one of the longest-lasting and most-widespread of all the empires in human history. Despite all this, the foreign policy principles and the political system of the republic that I have summarized above made it possible and even easy for Turkey to develop in a very short time friendly relations with all

Süha Umar *is a retired Ambassador of the Republic of Turkey. Early on in his career, he served in the Turkish Embassy in Buenos Aires, Consulate General in Burgas-Bulgaria, and Permanent Representations to the Council of Europe, NATO, and OSCE. He participated in the Law of the Sea Conference (UNCLOS), the Conventional Armed Forces Treaty (CFE), and the Middle East Peace Process. He was ambassador to Jordan and Serbia and served as the Director General for Bilateral Political Affairs of the Foreign Ministry.*

Photo: Guliver Image/Getty Images

Unveiled in 1964, Antalya's famed National Ascension Monument features a likeness of Atatürk

its neighbors, including Russia; prepared the ground for the establishment of the Balkan Pact in 1934 and the Saadabad (Sâdâbad) Pact in 1937 (the former was a treaty signed in Athens involving Greece, Romania, Turkey, and Yugoslavia; the latter was a treaty signed in Tehran involving Afghanistan, Iran, Iraq, and Turkey); resulted in Turkish membership in the League of Nations and then the United Nations, but also the Council of Europe and NATO; and ensured the launching of negotiations on accession to what became the European Union.

To the surprise of many, Turkey established good relations with Greece as soon as the War of Independence was over, even though it was that same Greece that, with the encouragement of the UK, had attempted to occupy western Anatolia in the hopes of making the Greek dream of the *Megali Idea* come true. This irredentist idea turned out to be a grave mistake for the Greek nation: it dearly cost Greece, the Greeks of the mainland, and the former Ottoman citizens of Greek descent that had for centuries lived in peace and harmony with Turks in Anatolia.

The bottom line is that from 1923 to 2002, Turkish foreign policy was based solely on the national interest and was independent at all costs. It used to be planned carefully, looking ahead twenty or thirty years into the future; we had foresight, predicted events correctly, and acted when the time was right and circumstances were ripe. And since it was widely understood that the achievement of foreign policy targets was predicated on a strong economy and a strong military—two elements that are, in fact, very much mutually-dependent—for decades Turkey did its utmost to have a growing economy and a reliable military to discourage any potential adversary from exercising its ambitions against our country.

The bottom line is that from 1923 to 2002, Turkish foreign policy was based solely on the national interest and was independent at all costs. It used to be planned carefully, looking ahead twenty or thirty years into the future; we had foresight, predicted events correctly, and acted when the time was right and circumstances were ripe.

The achievements of Turkish foreign policy between 1923 and 2002 are too numerous to get into in detail. But we can say that, overall, Turkish foreign policy proved its value for eight decades and served the best interests of the country. A few of the colossal achievements during this period can be mentioned: the Treaty of Lausanne (1923) which annulled for good the Treaty of Sèvres (1920) and made peace possible between Turkey and the Allied Powers; the Montreux Convention (1936) that established full Turkish sovereignty over the Turkish Straits and was beneficial to both the Black Sea coastal states and the world at large as one of the first confidence- and security-building measure ever formulated; the fact that Turkey kept itself out of the devastating Second World War; and, last but not least, the Cyprus Peace Operation (1974) that was launched when Greece attempted to annex the now-defunct Republic of Cyprus created by the London and Zurich Agreements (1959).

Of course, one might argue that taking part in the Korean War, in which Turkey fought side-by-side with the United States, and the Cyprus Peace Operation do not seem to be too compatible with a country claiming to have an anti-imperialist foreign policy. However, one should keep in mind that Turkey fought in the Korean War in order to be admitted to NATO (this happened in 1952), a reorientation that was the result of a unilateral decision by the Soviet Union in 1945 not to renew its Friendship and Cooperation Agreement (1925) with Turkey, while at the same time laying claim to the two easternmost cities of

Turkey (Kars and Ardahan) and asking for a high hand on the Turkish Straits. The Cyprus Peace Operation, on the other hand, had to be launched when Greece once again tried to expand its territory at the expense of Turkey by attempting *Enosis* or the unification of Cyprus with Greece, and only after Turkey had explored all other options for a joint action with the two other guarantor powers, the UK and Greece, to no avail. Here we also need to mention that in this period, any Turkish involvement in a military operation outside its borders was based on adherence to instruments of international legitimacy, such as a UN Security Council decision and/or an international agreement.

Snapshot in Time

Thus, when the AKP came to power in 2002, Turkey was a reliable and predictable partner in NATO. With its strong armed forces (fourth in NATO after the U.S., France, and the UK), Turkey was a country to reckon with for any adversary and reliable power when a need arose to form peacekeeping forces, fighting global terrorism, and so on.

In 2002, Turkey was also an active member with a good reputation in all pan-European and global organizations like the Council of Europe, the OSCE, the OECD, UNESCO, and the UN due to its wide-ranging political, economic, and cultural assets.

At the same time, Turkey as an "associate member" had a Customs Union Agreement with the EU and was expected to enter full membership negotiations. Turkey's Western orientation and shared values would have made this last mutually beneficial in many aspects—above all, to meet the challenges of our times that had been grouped together under Samuel Huntington's "clash of civilizations" moniker.

Moreover, Turkey had friendly relations with all the Balkan countries. It played an important role in the region in the wake of the Yugoslav civil wars and helped to make possible in many ways the soft transition for Bulgaria and Romania from membership in the Warsaw Pact to their joining NATO.

In addition, as a majority Muslim country with its secular democracy and its place in European and world politics, Turkey was a role model for nearly all Arab countries. The fact that Turkey was on excellent terms with Israel and all the Arab countries—except Syria (due to its support for the Kurdistan Workers Party (PKK) and its leader Abdullah Öcalan)—was also useful: its unique diplomatic posture enabled it to play an important role in the Middle East Peace Process in the wake of the Madrid Peace Conference (1991), especially in the Arms Control and Regional Security (ACRS) Group.

Lastly, after the disintegration of the Soviet Union, Turkey was able to establish close and fruitful relations with Azerbaijan and the Central Asian ex-Soviet republics, many of which had Turkish descendancy or, in one way or another, held an affiliation to the Turkish nation. Turkey was able to show the way and assist these newly-independent states to come into contact with Western institutions and organizations, including NATO.

Now, this too needs to be said. Turkey in those days had a carefully planned strategy and it handled its diplomatic initiatives and its cooperative relationship with the West in a professional manner, especially in the context of the Balkans and Eurasia. As a result, this posture did not prevent Ankara from having friendly and close relations with its powerful neighbor and historic adversary, Russia. This was the case even with regards to delicate issues, such as the 1990 Treaty on the Conventional Armed Forces in Europe (CFE)—one of the landmark documents of the end of the Cold War. Truth be told, Turkey had better cooperation and understanding on the part of the Russian Federation than with its NATO partners in the course of the CFE negotiations.

I am afraid all this is now history.

The Fall

When the AKP came to power in 2002, everything that constituted and governed Turkish foreign policy decisionmaking for nearly a century was put aside. If I were to describe the foreign policy of Turkey in the AKP era in one sentence, then it would be sufficient to say that it is decided, adjusted, and altered on a daily basis—sometimes even a few times in the course of a single day—according to the needs of Recep Tayyip Erdoğan: the AKP leader, former prime minister, and current (starting in 2014) President of the Republic of Turkey.

Since 2002, Turkish foreign policy decisions have been based on assessments made by people with insufficient knowledge and experience in the field of foreign relations.

Since 2002, Turkish foreign policy decisions have been based on assessments made by people with insufficient knowledge and experience in the field of foreign relations. Such people are neither able to properly read events and trends nor understand what is going on in the world; most of the time, they have a false perception what is the purpose of a country's foreign policy.

Even worse, most of the time foreign policy decisions and the initiatives that follow have been formulated and executed above all to satisfy and boost the ego of Erdoğan's domestic followers, under the guidance of Islam in general and one specific sect in particular (Sunni Islam).

In other words, since 2002, an influential and respected regional player has become "proactive" in foreign policy—in the words of Ahmet Davutoğlu, a former AKP foreign minister and prime minister. This led to Turkey oftentimes directly interfering in the domestic affairs of various countries in its neighborhoods, which almost always produced disastrous results—both for the countries in question and for Turkey itself.

Take the case of the Muslim Brotherhood. Especially after the Arab Spring, Erdoğan decided that the time had come for Turkey to lead the Middle East, thinking that the Muslim Brotherhood would come to power in most if not all Arab countries and that it would in turn accept Turkey under Erdoğan as its leader.

It did not take long for this surrealist dream to turn into a disastrous reality. Just about a year after Mohamed Morsi came to power following Hosni Mubarak's removal from office, the United States in particular and the West in general, which had for years promoted "moderate Islam" as an alternative to dictatorships in much of the Arab world, turned its back on Morsi by supporting Abdel Fattah el-Sisi's military coup d'état against him. This brought to an end the short-lived rule of the Ihvan-Muslim Brotherhood in the most important and influential of all Arab countries.

Moreover, the negative attitude of Saudi Arabia and most of the other GCC countries towards both the Muslim Brotherhood and Erdoğan's support for that Islamist movement led, in the end, to souring of relations with virtually every Arab country and Turkey's isolation in the Middle East.

Lastly, Erdoğan's support for the Muslim Brotherhood, coupled with his occasional comments in favor of jihad, did not help his reputation in either the East or the West. Suspicions of Turkey's intentions in both quarters grew, given the negative feelings and fears towards radical Islam were on the rise in important capitals around the world.

Then, of course, there is the Israel-Palestine question. Now, the State of Israel is a lasting reality in the Middle East as well as a crucial actor as far as peace and stability in the region is concerned. So is the State of Palestine. Even during the first few years of AKP rule in Turkey, Ankara was able to maintain balanced relations both with Israel and the Arab states. Such a relationship had many advantages—not the least of which was the ability to draw on what we can call its "convincing power," which was beneficial to both Israel and Palestine and perhaps more so to the latter.

However, as soon as Ankara adopted a foreign policy based on religious sectarian principles and opted for a one-sided approach to the Palestine question, Turkey's relations with Israel quickly deteriorated and the country lost its leverage with the Jewish state. When this attitude was coupled with Erdoğan's stand vis-à-vis Hamas, which defines itself as a branch of the Muslim Brotherhood, it afforded an opportunity for those that wanted to label Turkey as a country that supports terrorism to do so. In the meantime, Israel entered into new engagements with Arab states like Saudi Arabia, the United Arab Emirates, and Bahrain whilst relativizing its ties with Egypt and Jordan, both partners in the bilateral peace treaties with Israel. This had the consequence of further isolating Turkey in the region.

And then, of course, there is the Syrian affair. When President Bashar al-Assad was faced with the Arab Spring and his regime was destabilized on purpose by the United States, the AKP government made another crucial mistake: it joined the Obama Administration in order to prevent the establishment of a Kurdish entity in Syria after Iraq. This decision defied basic geopolitical logic, as Assad was the guarantor of the territorial and national integrity of Syria, which meant that he had a vested interest in keeping the Kurds under control, just as Saddam Hussein once did in Iraq. A united Syria under a strong central government was in the interest of Turkey and this had been proven when the PKK's Öcalan was obliged to leave Damascus and was captured in Kenya by Turkey before being tried and convicted of various crimes and jailed in 1999.

Contrary to the AKP's expectations, joint U.S.-Turkish intervention in Syria created a number of serious problems for Turkey. *First*, it precipitated the rise of ISIS. *Second*, it led to the de facto dismemberment of Syria. *Third*, it resulted in the YPG—seen by Turkey as a mere extension of the separatist PKK—becoming America's favored and highly-protected partner. And *fourth*, it contributed to the establishment of a Kurdish zone in northern Syria, east of the Euphrates River.

As time went by, Turkish military operations against Kurds in this zone created new difficulties in Turkish-U.S. relations, as these operations were seen by America as acting against its interest in Syria. Moreover, the Turkish military presence in northwest Syria—centered around Idlib—soon evolved into a thorny subject between Turkey and Russia and, to some extent, with Iran (Moscow and Tehran are Assad's two staunchest foreign supporters).

The Syrian affair also revived the historical rivalry between Turkey and Syria's best regional ally, Iran. At the same time, in an episode that surprised even most seasoned observers, Turkey and Brazil (at the time, both were UN

Security Council term members) tried to broker a nuclear fuel swap deal with Iran in an action that was perilously naïve at best or, as the West saw it, constituted an act supportive of Iran's clandestine nuclear activities that, I could add, should have been seen as a grave security risk by Turkey too, given its shared border with the Islamic Republic.

The Turkey-U.S. joint venture in Syria also gave a much-wanted opportunity to Russia to realize its centuries-long desire for unimpeded access to a warm sea. In this particular case, Russia's strong comeback to the Middle East and the Eastern Mediterranean ought also to have been seen more clearly for what it was from a national security perspective: the attempted encirclement of Turkey from the south.

The disastrous Syrian affair proved once again the veracity of the most basic rule of a foreign policy: to keep a country's options open. The AKP's failure to do so represents a further stinging indictment against the manner in which it has conducted Turkish foreign policy since 2002.

The disastrous Syrian affair proved once again the veracity of the most basic rule of a foreign policy: to keep a country's options open. The AKP's failure to do so represents a further stinging indictment against the manner in which it has conducted Turkish foreign policy since 2002. Erdoğan's recent futile efforts in New York and Sochi to mend ties with both the U.S. and Russia in September and October 2021, or at least to play these two against each other without any success, clearly showed that AKP's foreign policy had left Turkey with no option at all. And thus, alas, Turkey could be said now to be helpless—certainly no longer a master of its own fate.

Neo-Ottomanism and the West

Another aspect of Turkey's new approach to foreign relations is predicated on the idea that harking back to its Ottoman imperial past, which purposefully had not been done since 1923, provided it with a sort of "strategic depth"—based on an accumulation of necessary knowledge and experience—to enable it to play a determinant role in the Middle East and the Balkans.

This approach was also introduced by Davutoğlu. In a 2013 speech, for instance, he indicated that

> the last century was only a parenthesis for us. We will close that parenthesis. We will do so without going to war, or calling anyone an enemy, without being disrespectful to any border; we will again tie Sarajevo to Damascus, Benghazi to Erzurum to Batumi. This is the core of our power. These may look like different countries to you, but Yemen and Skoplje were part of the same country a hundred and ten years ago, as were Erzurum and Benghazi.

Again, this approach, introduced by Davutoğlu to the Turkish public even before he entered politics, was readily adopted by Erdoğan. The problem was that the Ottoman period was perceived and termed by the countries of the aforementioned regions—nearly all of which had spent centuries under Ottoman rule—as "Neo-Ottomanism."

Thus, the problem with this aspect of AKP foreign policymaking is that it overlooks the simple fact that both in the Balkans and the Middle East, the Ottoman legacy does not have a good reputation: this period is, by and large, deplored and even detested in the historical narratives of the relevant nations; they believe that the Ottoman period is a principal reason for why they now lag behind the developed world. This may or may not be true, but the fact is that, just like old habits, old beliefs and old perceptions die hard.

One final point on this: when Ankara tried to use local muftis and the President of the Directorate of Religious Affairs of Turkey (the state institution is known as the Diyanet) to conduct its foreign policy in the Balkans, eyebrows were raised even in those parts of Bosnia in which the Ottoman heritage is positively perceived.

Things have also not gone well for Turkey in the West. When Turkey purchased S-400 air defense systems from Russia in 2017—it is believed to have been a compensation for the Russian fighter jet downed by the Turkish air force at the Turkish-Syrian border in November 2015—the United States reacted negatively, irrespective of the fact that the system has never been made operational. Turkey was then left out of the U.S.-led F-35 Fighter Project notwithstanding the fact that it was a joint producer of the aircraft; Turkey was also made subject to sanctions by the U.S. under its 2017 Countering America's Adversaries Through Sanctions Act (CAATSA). Russia did not miss the opportunity and tried to drive a wedge between Turkey and the West, thus weakening NATO solidarity while keeping Turkey under constant pressure in theatres like Syria.

Even though Turkey, as a NATO partner, had in the past tried to obtain cutting-edge Western air defense systems—for instance, America's Patriot system—but had been refused, still the acquisition of S-400 air defense systems led to an even deeper questioning by NATO. The handling of this issue by Erdoğan and the AKP—notwithstanding the fact that Turkey actually had a good and defendable reason for acquiring the Russian system—was so far from being professional that some NATO allies even went as far as to claim

that Turkey was departing from her NATO allegiance. This perception—no matter how false it may be—was counterproductive, to say the least, in instances in which Turkey needed to have NATO partners by its side. A good recent example of this the delimitation of the continental shelf and the exclusive economic zone in the Aegean and the Eastern Mediterranean.

The AKP used the EU as a leverage to change the secular and democratic political system of Turkey whilst the EU uses these same changes as a pretext to block Turkey's EU accession process while fully supporting Kurdish separatist ideas in order to make Turkey more "digestible".

Relations with the EU did not fare better either. During its first years in power, the AKP gave the impression that it was for "democracy," adhered to "European values," and would cooperate with the EU on various issues. It did indeed, certainly at the onset, but primarily to solidify its power and to, if not totally eliminate, at least weaken the country's longstanding institutions. Special emphasis was placed on the Armed Forces, so as to avoid the possibility of a coup against the AKP.

At the onset, certainly, the EU happily gave its full support to this and similar AKP policies, which had as their effect the distancing of Turkey from what the new leaders in Ankara most feared, namely Kemalism. This was a two-way game deliberately played by the EU on one side and the AKP on the other: the AKP used the EU as a leverage to change the secular and democratic political system of Turkey whilst the EU uses these same changes as a pretext to block Turkey's EU accession process while fully supporting Kurdish separatist ideas in order to make Turkey more "digestible"—a term frequently mentioned even in official EU circles since 2015.

Precious Solitude? Valuable Loneliness?

The record of the AKP's conduct of Turkish foreign policy since 2002 is clear: deteriorated relations countries, both East and West, coupled with the posing of challenges to leaders of the major powers. This was done for no apparent logical strategic reason save for acquiring and maintaining domestic popularity.

The cumulative result of all this is that Turkey now finds itself in a state of "precious solitude" or "valuable loneliness," as Davutoğlu once put it. However, no matter how romantic and attractive the label may be in some domestic circles, Turkey is more and more isolated; this has made defending even its most vital national interests more difficult.

Take for example the Aegean and the Eastern Mediterranean, as mentioned briefly above. The United States and the EU openly took the side of Greece against Turkey on the issue of the continental shelf in the Aegean. Similarly, despite the fact that Turkey has the longest coast in the Eastern Mediterranean, nearly all the coastal states of the region (Syria, Israel, and Egypt) signed continental shelf and exclusive economic zone delimitation agreements with Greece and the Greek Cypriot Administration of South Cyprus. Turkey was able to reach a disputable deal only with Libya.

The record of the AKP's conduct of Turkish foreign policy since 2002 is clear: deteriorated relations countries, both East and West, coupled with the posing of challenges to leaders of the major powers.

The effectiveness of the foreign policy of a country can be measured; and the most relevant measuring stick is the rate of success a country has in achieving its national interests. In this short evaluation, I have tried in earnest to tell the story of the rise and the fall of Turkish foreign policy since 1923. I leave it to the readers of *Horizons* to decide whether Turkey under the AKP has conducted a considered and successful Turkish foreign policy. To provide an affirmative answer, the reader would need to explain what exact national interest Turkey has achieved since 2002.

Change and Continuity in Turkish Foreign Policy

Reconceptualizing Turkey's Role as a Rising Power in Regional Politics

Sinan Ülgen

TURKEY is approaching a critical electoral threshold. By mid-2023 at the latest, the Turkish electorate will go to the polls for a combined presidential and legislative elections. Recent polls indicate that the ruling Justice and Development Party (AKP) is losing support and the electoral race is now wide open.

In other words, it is becoming increasingly likely that Turkey will witness political change, which could have significant implications not only for domestic politics but also foreign policy.

It will therefore be important to evaluate the nexus of change and continuity for Turkish foreign policy in the years to come. This evaluation will firstly require a stock taking.

From a Hopeful Beginning ...

The past two decades of AKP rule was marked by three different foreign policy proclivities. The first decade is properly viewed as a continuation of Turkey's legacy foreign policy outlook, as the newly established political leadership espoused similar goals as previous administrations. For instance, the strengthening of Turkey's ties with its transatlantic partners was a core objective—in particular, a focus was maintained on EU membership.

Consequently, in the wake of a series of critical domestic reforms, Turkey was finally granted the green light to initiate accession negotiations with the EU in 2004. Regionally, Turkey strove to leverage its position as a reliable, geostrategic, partner acting as a bridge between the West and constituencies in the

Sinan Ülgen *is a Visiting Scholar at Carnegie Europe in Brussels and the Executive Chairman of the Istanbul based EDAM think tank. You may follow him on Twitter @sinanulgen1.*

Photo: Guliver Image/Getty Images

Today's architects of Turkish foreign policy: Mevlüt Çavuşoğlu and Recep Tayyip Erdoğan

Middle East. It is during those years that Ankara engaged in careful diplomacy to nurture improved ties with Syria, and also acted as a mediator in long standing divisions between Israel and Syria.

Furthermore, in this period, the country's foreign policy outreach was helped by a burgeoning economy and, as a result, Turkey could contemplate enriching its soft power instruments. Gradually, the country was able to become a more important actor in international development and humanitarian assistance. The Turkish Cooperation and Coordination Agency (TIKA) became engaged in a growing number of regional assistance projects. Turkish Airlines initiated its ambitious journey to grow its international network, gradually transforming Istanbul into a global air transport hub. The success of Turkish soap operas enhanced Turkey's international image. And, thanks to the leadership of three successive foreign ministers (Abdullah Gül, Ali Babacan, and Ahmet Davutoglu), during this period the Turkish diplomatic network expanded, eventually becoming the fifth largest in the world, overtaking even France and Germany.

In short, in the first decade of this century, the Turkish leadership was able successfully to combine the continuity

in the main tenets of its foreign policy with elements of change and innovation in its diplomatic practice. The end result was the transformation of Turkey into a more visible and potent actor on the world stage.

Two examples best illustrate this phenomenon. After a 48-year absence, in 2009 Turkey was elected to term membership in the UN Security Council. Moreover, Turkey's transformation rekindled global interest in the "Turkish model." As a country that had successfully combined democracy, modernity, economic growth, and Islam, Turkey became a source of inspiration for the Arab states that, it was predicted, were well-positioned to accomplish a seamless transition to democracy in the wake of the Arab Spring.

In the first decade of this century, the Turkish leadership was able successfully to combine the continuity in the main tenets of its foreign policy with elements of change and innovation in its diplomatic practice.

Paradoxically, it was that same Arab Spring, which was triggered in late 2010 by events in far-off Tunisia, that ultimately upended Turkey's foreign policy strategy. The Turkish leadership saw in the Arab Spring an unalloyed opportunity to elevate the country's regional influence. This vision provoked a clear break with Turkey's past behavior and marked a new beginning for its international diplomacy.

Thus began the second era of the AKP-led Turkish foreign policy, shaped firstly by a reconceptualization of Turkey's identity and its potential role as a diplomatic actor. During much of his time as Foreign Minister, Ahmet Davutoglu led this intellectual effort and received the backing of then-Prime Minister Recep Tayyip Erdogan in this challenging, ambitious, and yet, ultimately unsuccessful endeavor.

The main driver of this change was ideology. Namely, Turkey's ruling political elites wanted to redirect the country's foreign policy to reflect the changing nature of the domestic political landscape. At the core of this thinking was the understanding that since the early Republican years, Turkey had been forced to follow the West in ways that were inimical to its national interests. Such a one-dimensional alignment was largely due to the geopolitical circumstances of the Cold War, but also because Turkey's generations of then-secular leaders wanted the alliance with the West to work. They envisioned this alignment with the West as a tool to complete the transformation of Turkish society and the adoption of Western social norms. These included secularism and gender equality, and constituted part of the core of Kemalism and a legacy of the Atatürk-era reforms.

Yet, from the perspective of the AKP leadership, this categorical and virtually unconditional alliance with the West was antithetical to centuries of the country's heritage. As the successor nation of a great empire, an economically emboldened Turkey should have been able to move beyond these limits and adopt a more independent foreign policy that was more aligned with its Muslim and Ottoman heritage.

The geopolitical consequences of the end of the Cold War, combined with the prospect of democratic upheavals in Turkey's southern neighborhood, supported the option of a more strategically autonomous foreign policy.

In contrast to the ideational role of foreign policy in the Republican years, Turkey's new foreign policy—which came into life after the first decade of AKP rule—was to support a societal ideal that was more influenced by religion and socially conservative values. In addition to this more domestically-shaped narrative, changes in the international system had also seemingly provided an opening for a more ambitious Turkish foreign policy. The geopolitical consequences of the end of the Cold War, combined with the prospect of democratic upheavals in Turkey's southern neighborhood, supported the option of a more strategically autonomous foreign policy. Thus was the Turkish leadership enthused by the potential of being in the driver's seat of what it perceived as being an inevitable historical transformation of the region.

...TO THE CHALLENGE OF STRATEGIC AUTONOMY

The second phase of the AKP era was thus characterized by more ambitious foreign policy goals that were to be pursued in increasingly confrontational theaters. Despite this difficult backdrop, the new narrative of an influential Turkey becoming a cornerstone of the new regional order captivated the imagination of the country's domestic audience. After years of accumulated frustrations in the country's dealings with the West—in part stemming from the perceived duplicity and double-standards of the EU—the domestic constituency was ready to embrace the espousal of a more ambitious rhetoric defining the new Turkey and its international role.

The first radical departure from the traditional tenets of Turkish foreign policy was Syria. After having unsuccessfully striven to convince the regime

headed by Bashar al-Assad of the need for political reform, Turkey changed tack and embraced an agenda of regime change. The case of Syria represents the first time in history that Ankara used its power to attempt to oust a regime in a neighboring state.

The Turkish government became part of a large campaign that involved support to civilians but also armed opposition groups in Syria. The hope was that the Assad regime would quickly succumb to a combination of domestic and international pressure and would, in short order, be replaced by political actors benefiting from the support of the majority Sunni population of Syria. It was on the basis of such an understanding that led the Turkish authorities also to adopt an open-door policy to Syrian refugees. After all, the thinking went, Assad had only a few weeks left in power. The more the Syrian regime proved resilient—thanks in no small part to the provision of support by Iran and Russia—the more Turkey became a safe haven for a growing number of refugees from Syria. As a result, Turkey today hosts the largest number of refugees in the world.

The case of Syria represents the first time in history that Ankara used its power to attempt to oust a regime in a neighboring state.

The second manifestation of Turkey's abandonment of its traditional foreign policy principles was the newfound willingness of its leadership to better position the country in the middle of internal political struggles taking place in foreign states. The ruling AKP had established close relations with various political movements in the region that all traced their roots back to some form of political Islam—with the Muslim Brotherhood being a case in point. The hope was that these movements would rise to power in their respective countries, leading Turkey—as their strong backer— to become the dominant external actor in each of them.

In hindsight, what should have remained a political party strategy was transposed full-on into state policy. Consequently, Turkey found itself a party to the internal disputes of foreign countries. In Egypt, for instance, Turkey was seen to be very supportive of the Muslim Brotherhood-led Mohamed Morsi government. Once Morsi was ousted after little over a year in office, Turkey's relationship with the succeeding Egyptian government, headed then and now by Abdel Fattah el-Sisi, was deeply tainted. Furthermore, the evident support to political movements linked to the Muslim Brotherhood was also at the core of Turkey's damaged relations with the Gulf states (except for Qatar).

The third point of departure relates to the nexus between domestic politics and foreign policy. For a long time, foreign policy in Turkey was viewed as being almost hermetically sealed from domestic political considerations. Foreign policy decisionmaking had been under the prevailing influence of the Foreign Ministry, which was staffed almost exclusively by professional career diplomats. The military was also an influential actor in areas of strategic relevance. The political leadership had the final say, sure, but it was essentially swayed by the calculations, assessments, and recommendations of these two powerful, professional institutions.

Regardless of whether Turkey ends up with a different constellation of political leadership after the critical 2023 elections, Ankara's self-assessment of being a rising power in a multipolar world will be a permanent fixture of Turkey's future diplomacy.

Under the AKP, the balance of power shifted to politicians—to the detriment of the institutional players. In many ways, Turkey lurched from one extreme to the other. In the olden days, the body politic was heavily influenced by institutional thinking, with little interest in the domestic impact of their calculus. In the new Turkey, the body politic wanted no institutional pressure. Foreign-policy-making disassociated itself from the "weight" of these institutions and increasingly became guided and even led by domestic political concerns. The shift away from a parliamentary system and back to a presidential one as a result of a April 2017 constitutional referendum accentuated these negative changes and further usurped the institutional underpinnings of Turkish foreign policy. Decision-making became opaquer and increasingly driven by a close set of presidential advisors.

As a result, Turkish foreign policy became less predictable, changing its agenda in accordance with fast-moving domestic objectives. This shift was accentuated by a change in the foreign policy rhetoric as well. The highly-polarizing and combative language of Turkish domestic politics began to permeate the country's foreign policy discourse. The public speeches of the Turkish leadership had made foreign countries and leaders just as much of a target as domestic opposition figures.

Unsurprisingly, the end result of these radical departures from the traditional tenets of Turkish foreign policy proved to be detrimental to Turkey's aspirations to project its prestige, influence, and power in its neighborhood(s). In fact, Ankara became more isolated and its relations

with established partners in the West became increasingly antagonistic.

All this finally compelled the current leadership to recalibrate its approach to Turkish foreign policy. The rhetoric towards the United States and the EU became less incriminating and combative. Ankara has also undertaken de-escalation measures in the Eastern Mediterranean. Diplomatic openings were initiated with a view to improving bilateral relations with the region's countries including Israel, Egypt, and the UAE—even some type of normalization with Armenia appears to be on the horizon. It is the form and longevity of this recalibration that will determine the future trajectory of Turkey's diplomacy.

The end result of Turkey's tarnished ties with its traditional allies in the West and its neighborhood(s) have demonstrated the limits of the illusion of Ankara's strategic autonomy.

Looking to the Next Decade

Turkey's foreign policy inclinations in the next decade will essentially be determined by how its political leadership will decide to conceptualize the country's role as a rising power. A major element of continuity in Turkey's international relations will therefore be its self-perception of its new role. Regardless of whether Turkey ends up with a different constellation of political leadership after the critical 2023 elections, Ankara's self-assessment of being a rising power in a multipolar world will be a permanent fixture of Turkey's future diplomacy.

As briefly examined in this essay, this identity has been interpreted over the past decade in a way that encouraged unilateralism. Turkish policymakers intended to demonstrate both domestically and to outside actors that the country had acquired the capability to conduct an independent foreign policy. The tensions inherent to this type of accentuated unilateralism further complicated policymaking and undermined the traditional alliances of a country already exposed to the many instabilities stemming from the Middle East. But these tensions also played an important role in nurturing a domestic narrative about Turkey's indomitable rise and the negative reactions of outside powers that wanted to constrain and contain Turkey's foreign policy activism and autonomy.

The end result of Turkey's tarnished ties with its traditional allies in the West and its neighborhood(s) have demonstrated the limits of the illusion of Ankara's strategic autonomy. Indeed, despite its aspiration, Turkey remains firmly anchored in the Western community of nations. In addition to being a NATO member, over 40 percent of the country's exports are destined for EU member states and another 6 percent or so each to the UK and the United States. In addition, Turkey gets most of its foreign direct investment (FDI) and technology from Western countries. EU member states account for almost 70 percent of all incoming FDI, with another nearly 10 percent accounted by the United States.

A new balance will have to be found between the need for a democratic government that is accountable to its electorate and the need for a more mature and predictable foreign policy.

Against this backdrop, the 2020 economic downturn, compounded by a sharp drop in FDI, a negative foreign investment balance sheet (excluding real estate), and a lowering of credit risk scores—and, more recently, a spike in inflation and a downturn in the value of the national currency—are to be associated with these frail political relations.

The next phase of Turkey's foreign relations paradigm will therefore be marked by how well the country's growing capabilities—but also its ambitions—can be reframed to allow for a more cooperative foreign policy pattern. This objective will in turn require three fundamental changes.

The *first* is the decoupling of foreign policy from domestic political considerations. A new balance will have to be found between the need for a democratic government that is accountable to its electorate and the need for a more mature and predictable foreign policy. This new understanding should be instrumental in containing the proclivities of the ruling elites to instrumentalize foreign policy for domestic goals.

This objective will be greatly facilitated by a *second*, namely the re-institutionalization of foreign policy. As discussed above, the transition back to a presidential system has led to the erosion of the role of traditional institutions (e.g., ministries) in the policymaking process—to the benefit of the presidential administration. This is also true of foreign policy, where the role of the Foreign Ministry has been diminished. This domain requires rebalancing, which would reempower the traditional institution of policymaking. Such a rebalancing would improve the predictability of Turkey's foreign policy, as the heavier weight of the relevant institutions could more effectively counter the tendencies fueled by exclusively domestic political considerations.

Third, the country's foreign policy retransformation will be more effective if Turkey's partners respond positively to such an agenda of change. The United

States and the EU—Turkey's strategic allies in the domains of security, defense, and economy—can help Ankara in its bid to develop a new understanding of how Turkey, as a rising power, can prioritize positive sum scenarios. For instance, Washington will need to alter its approach and start to engage constructively with the Turkish leadership to tackle the corrosive set of bilateral problems, including the ongoing U.S. relationship with the PKK-linked Syrian PYD and the dysfunctionalities in defense industry cooperation. At the same time, the EU will need—at the very least—to cease its obstructionism regarding the launch of an ambitious trade agenda and endorse the start of the negotiations for a modernized Customs Union between Turkey and the EU. The outcome of new negotiations to reach a fair and lasting model of cooperation on the refugee issue will be of equal importance.

At bottom, what is at stake in the next decade is the identity of Turkish foreign policy. A departure from what marked the past decade—unilateralism inspired by a strong yearning for strategic autonomy—is already under way. This change in approach is evident in the more recent efforts at diplomatic rapprochement with allies and regional partners. Ultimately, the success of this transformation will be conditional on a clear demonstration of intent by the country's leadership that Turkey, as a rising power, needs to establish a more constructive and cooperative relationship with its main allies.

A departure from what marked the past decade—unilateralism inspired by a strong yearning for strategic autonomy—is already under way.

HIGH TIME FOR DIALOGUE IN THE EASTERN MEDITERRANEAN

Mustafa Çıraklı

THE exploration and discovery of offshore natural gas resources in the waters of the Eastern Mediterranean over the past two decades has been quickly followed by a resurgence in territorial disputes. This has turned the basin into a ticking geopolitical time-bomb that carries the potential for spiraling into a regional conflict with important spillover effects for Transatlantic relations.

More specifically, the lack of an agreement concerning the exploitation and equitable sharing of these resources, inextricably linked to the unresolved "Cyprus problem" and the competing claims over maritime jurisdiction areas between Turkey, Greece, and the Republic of Cyprus (RoC) has increased the chances not only for a dangerous Greek-Turkish clash. It has also increased the likelihood of a weakening of the Western alliance through an emboldened France ready to draw a separate course from NATO, both by taking sides in such a conflict and in relation to wider European security.

Turkey, for its part, has on numerous occasions called for an "Eastern Mediterranean Conference" to resolve pending issues and outstanding conflicts through peaceful means. In the same vein, the country's foreign minister, Mevlüt Çavuşoğlu, reiterated that there are indeed only two choices: lock horns or find a "win-win formula" to define a mutually-beneficial way forward.

While an international conference may not deliver a panacea—given the multiple points of contention—diplomatic engagement would still help stabilize the Eastern Mediterranean through the resumption of dialogue. Seeking to contain the crisis, Turkey has already shown restraint in its response to what it views as the violation of its sovereign rights. With the encouragement of the United States and its European partners, Turkey also resumed exploratory talks with Greece and continues to explore backdoor channels to normalize strained relations with regional neighbors (with some success), including Israel and Egypt—the two countries that have expressed reservations toward the Turkish calls for the multilateral conference on the Eastern Mediterranean when the president of the European Council, Charles Michel, floated the idea in late 2020.

Photo: ?????????

The Eastern Mediterranean basin

But Turkey needs more support and assurance to sustain its tentative de-escalatory approach. A renewed effort now by Washington and Brussels toward convening the aforementioned conference would go some way toward it.

A DANGEROUS STANDOFF

Turkey's activities in the Eastern Mediterranean are based on a maritime agreement signed with the Turkish Republic of Northern Cyprus (TRNC) in 2011 and with Libya's former Government of National Accord, which allowed Turkey to re-draw the EEZ and continental shelf zone boundaries within the Eastern Mediterranean.

Mustafa Çıraklı *is an Associate Professor of International Relations and Director of the Near East Institute at Near East University.*

The Turkey-Libya deal is widely dismissed by Greece and the RoC—but also by France and Egypt—as null and void. Licenses granted by the TRNC are also disputed, with the position of both Greece and the RoC being that the TRNC, which they and many other states consider to be a breakaway entity, has no authority to issue licenses.

The Eastern Mediterranean basin is a ticking geopolitical time-bomb that carries the potential for spiraling into a regional conflict with important spillover effects for Transatlantic relations.

Moreover, from a Greek and Greek Cypriot perspective, Ankara is to blame for the current escalation of tensions resulting from Turkey's decision to pursue its own exploratory activities in the region. Asserting Greek claims to sovereignty over most of the Aegean, Greece and the RoC also accuse Ankara of illegally operating within each of their respective Exclusive Economic Zones (EEZ). The RoC's position is that it has a sovereign right to explore and develop all the island's natural resources since it is the sole legal and legitimate government of all of Cyprus. In that vein, the Greek Cypriot government has been raising its objections with both the United Nations and the European Union (EU) over Turkey's gas exploration and drilling activities in Cypriot waters, claiming that Turkish actions violate its sovereign rights. The RoC has also pointed out that "all Cypriots" would benefit from revenue that may come from drilling under its aegis. To that end, Nicosia has offered Turkish Cypriots a share of possible gas revenues, should Ankara recognize the RoC's sovereign rights over the island's energy resources.

For Turkey though, the territorial claims of both Greece and the RoC are groundless, with Turkish officials accusing both Athens and Nicosia of trying to exclude Turkey and its Turkish Cypriot kin from reaping the benefits of the region's oil and gas findings. Also, the TRNC argues—as does Turkey—that the Turkish Cypriots have equal rights and should have a say in managing the island's resources, independently of the outstanding Cyprus problem. To be more exact, Turkey objects to the EEZ claims of the Greek and the Greek Cypriot sides on the grounds that, *one*, these claims deny the co-ownership rights of the Turkish Cypriot community; *two*, they do not respect the rights and interests of all stakeholders; and *three*, they distort the equitable delimitation of maritime boundaries under the principles of international law.

On the Aegean meanwhile, the ensuing war of words between Turkey and Greece over maritime rights nearly came to boiling point during the first summer of the COVID-19 pandemic. On 21 July 2020, Turkey announced that it was sending its *Oruç Reis* research ship to carry out a seismic survey in the South-eastern Aegean Sea claimed by both Turkey and Greece as part of their respective sovereign continental shelfs. A series of escalating moves and countermoves led to the longest and most fractious standoff between the two NATO allies in over 20 years.

Nicosia has offered Turkish Cypriots a share of possible gas revenues, should Ankara recognize the RoC's sovereign rights over the island's energy resources.

A breakthrough appeared on 8 October 2020 when the two sides agreed under Germany's mediation and with the full U.S. blessing, to resume exploratory talks for resolving their maritime disputes. But a few days later, on 11 October 2020, Turkey withdrew from the talks and released a NAVTEX—or a navigational warning—that it would be conducting surveys on the waters 6.5 nautical miles off the Greek island of Kastellorizo, which is located a few kilometers off the southwestern-most point of Turkey's Turquoise Coast. After a brief battle of heated exchanges, another space opened for resuming exploratory talks when Ankara pulled back the *Oruç Reis* from the disputes zone in late November 2020 and announced a month later that the vessel would carry out seismic research in uncontested waters until 15 June 2021. In January 2021, following a meeting of delegations in Istanbul, the two sides announced that the high-level contacts would continue in Athens.

Tensions were ramped up again in March 2021, however, when an unexpectedly volatile press conference between the two countries' foreign ministers, Mevlüt Çavuşoğlu and Nikos Dendias, saw the two men trading accusations on maritime borders, migrants, and the treatment of minorities. Calm was ensued after a more amicable meeting in May 2021 during Çavuşoğlu's visit to Athens, which saw the two sides announcing that they had agreed to work together for better ties.

More recently however, on 18 September 2021, fresh tensions were sparked after Turkish frigates stopped the Italian-operated vessel *Nautical Geo* from conducting surveys on Greece's behalf, 6 miles off the Greek island of Crete. Turkey subsequently asserted that it would resume its own surveys if the RoC proceeds with its planned drilling by the end of 2021. In early December 2021, Turkey threatened to block any unauthorized search for gas and oil in its economic exclusive zone in the eastern Mediterranean after the RoC awarded hydrocarbon exploration

and drilling rights to a venture of Exxon Mobil and Qatar Petroleum in an area that lies in part in what Turkey claims is a part of its continental shelf.

ANKARA'S CONUNDRUM

Bickering over Eastern Mediterranean maritime boundaries were initially a local affair, revolving around competing sovereignty claims among the RoC, Greece, and Turkey. During the past six years however, the region's offshore natural gas resources have witnessed high-stakes geopolitical jockeying not only among the three Mediterranean countries themselves, but also other littoral states and outside international actors.

Bickering over Eastern Mediterranean maritime boundaries were initially a local affair, revolving around competing sovereignty claims among the RoC, Greece, and Turkey. During the past six years however, the region's offshore natural gas resources have witnessed high-stakes geopolitical jockeying.

A key turning point in this regard was the August 2015 discovery of Egypt's *Zohr* natural gas field by the Italian energy giant Eni. Eni's *Zohr* discovery, considered to be the largest Eastern Mediterranean gas find to date, increased the prospects that some of it could be exported. Eni, which is also the lead license-holder in the RoC's gas fields, then began to drum up support for a plan to pool Egyptian, Cypriot, and Israeli gas and to fast track production by utilizing the existing natural gas infrastructure in Egypt —where it also holds a large equity share—to export it to the European Union as liquified natural gas (LNG).

Irked by the idea that it was no longer considered the only export hub for the Eastern Mediterranean gas, Turkey retaliated through a limited naval action. On 23 February 2018, the Turkish navy blockaded an Eni drillship before it could reach its destination on the east coast of Cyprus, forcing the vessel to withdraw. Eni responded by striking a partnership with the French energy giant Total in all its seven Cypriot licensing blocks, a move that catapulted France into the middle of the Eastern Mediterranean energy landscape.

Then, in March 2019 leaders from Greece, Cyprus, and Israel—with U.S. Secretary of State Mike Pompeo at their side—signed an agreement on the proposed "EastMed pipeline." The project took on institutional form in September 2020 when the Eastern Mediterranean Gas Forum (EMGF) was established as an international organization by Greece, Cyprus, Egypt, Israel, Italy, Jordan, and the Palestinian Authority. The final step

to setting up the EMGF and its Cairo HQ was cleared after Egypt ratified its founding charter in October 2019. Turkey has insisted that it was left out purposefully and has blamed the EMGF for taking Greece and Cyprus's side.

Also alarming for Ankara, in December 2019, U.S. President Donald Trump signed the Eastern Mediterranean Security and Energy Partnership Act, which put Greece and the RoC at the forefront of US policy in the region—a role historically played by Turkey.

This was the context in which Turkey shifted in its foreign policy preference towards a more assertive diplomatic posture in the Mediterranean basin. Turkey expressed its displeasure at these developments by engaging in a series of limited countermeasures (e.g., sending exploration and drill ships into Cypriot waters, with naval escort). In late 2019, Ankara also signed a security and maritime border agreement with the Tripoli-based Government of National Accord, which was followed by the deployment of Turkish troops against the Haftar forces backed by the UAE, France, and Russia. Most remarkably, the new maritime border agreement introduced a vertical line across the Mediterranean: it re-drew the EEZ and continental shelf zone boundaries and marked the Turkish-Libyan economic zone. The aim was to delay the pipeline plans put forward by Greece, Cyprus, Egypt, and Israel.

Another Turkish grievance relates to the situation in Cyprus. There is a growing conviction in Turkey that the RoC's refusal to discuss Cypriot gas resources with the Turkish Cypriot side reflects a wider Greek Cypriot unwillingness to accept the Turkish Cypriots as co-equal partners in government. The general mood in Turkey also seems to be that Turkey and the Turkish Cypriots did what they could and that the proposals they tabled, together with the TRNC, for the joint development of the island's natural gas resources gave the Greek Cypriots ample room for compromise. Successive rounds of talks—held in 2017 and 2018 between the two sides, along with the guarantor nations of Greece, Turkey, and the United Kingdom—ended in deadlock. Turkish and Turkish Cypriot warnings regarding what they saw as unfair actions by the RoC fell onto deaf ears. At that point, Ankara began trying to counter these developments by acquiring research and drilling ships and sending them, often with naval escorts, into contested waters.

From a security perspective too, Turkish actions are not surprising. Turkey aspires to have regional clout, and hosting the Eastern Mediterranean pipeline would cement that. But its positioning within the Eastern Mediterranean energy landscape is also strategically important for the country's geopolitical reach, and for its ability to act. In this sense, Turkey confronts the possibility

that joint action by the Greek and Egyptian navies could, in theory, close off the Mediterranean to Turkey by forming a blockade from the outer islands of the Dodecanese (Rhodes, Karpathos, Kasos) to Crete and then to the North African coast at the Eastern Libya/Western Egypt border region.

The French Connection

In the same vein, Ankara sees the initiation of a new, anti-Turkish axis (with France at its helm) in two other developments, aside from the deepening security cooperation between the Mediterranean countries: the trilateral RoC-Greece-Egypt defense relationship and the strengthening military cooperation between the RoC, Greece, and France. Turkish President Recep Tayyip Erdoğan's recent assertion that "it is absolutely not a coincidence that those who seek to exclude us from the eastern Mediterranean are the same invaders as the ones who attempted to invade our homeland a century ago" underscores such Turkish anxieties of being 'boxed up' or put under siege.

Turkey aspires to have regional clout, and hosting the Eastern Mediterranean pipeline would cement that. But its positioning within the Eastern Mediterranean energy landscape is also strategically important for the country's geopolitical reach, and for its ability to act.

Moreover, France's involvement in the Eastern Mediterranean is viewed by Ankara as a reflection of the French desire to fill the power vacuum created by decreasing American interest in the Middle East and Mediterranean basin as the latter shifts its focus to threats in the Asia Pacific. Examples include the fact that it is deepening its strategic and defense cooperation with the regional actors; sending its warships and planes to take part in joint exercises with Greece and Cyprus; and is venturing its research vessels (together with naval escort) into disputed waters.

It is no secret that the French President Emmanuel Macron has the ambition to restore France's power and leadership over the Mediterranean, an area that Paris considers as part of its traditional sphere of influence. In the spirit of his predecessors' projects for the southern European neighborhood, President Macron wishes to set a *Pax Mediterranean*: a regional Mediterranean order that gravitates around Paris.

But perhaps the bigger judgment here—one that has gone relatively unnoticed so far—is whether the French involvement in the Eastern Mediterranean is only about the gas reserves (i.e., protecting Total's interests) and curbing Turkish influence in the Eastern Mediterranean; or whether it is instead driven by the wider quest to redesign Transatlantic relations, and, by extension, Europe's security architecture.

In this regard, the defense pact that Paris signed with Athens in October 2021, hard on the heels of the AUKUS submarine fallout, can be seen as a worrying indication that French plans in the Eastern Mediterranean parallel its efforts to consolidate European military structures such as EUFOR (European Union Force) or the PESCO (Permanent Structured Cooperation). Macron has so far insisted that the Franco-Hellenic deal—first of its kind to originate from within NATO—is not "an alternative to the United States alliance." His assertion that the move is needed to "take responsibility of the European pillar within NATO" also appears to be in sync with the longstanding U.S. position regarding "burden sharing."

France's involvement in the Eastern Mediterranean is viewed by Ankara as a reflection of the French desire to fill the power vacuum created by decreasing American interest in the Middle East and Mediterranean basin as the latter shifts its focus to threats in the Asia Pacific.

Yet, it is the subtext that matters here. As one seasoned observer puts it: "Macron is the man who described NATO two years ago as 'brain dead.' He will not have changed his mind now."

It is true that the Trump Administration maintained a rather aggressive attitude toward the Atlantic Alliance, and the realization on the part of France that "Europeans must step up" is not bad news. Having said that, a hastily drawn plan for "strategic autonomy" on the back of ongoing disputes among NATO allies carries the risk of detaching Europe from the United States.

Will Germany Step Up?

Until now, the EU's engagement with the Eastern Mediterranean was overshadowed by France, Greece, and the RoC, on the one hand, and marked with an unrelenting focus on its volatile relationship with Turkey, on the other.

While Turkey's actions in the region—and around Cyprus in particular—are seen in many European capitals as both an example of "gunboat diplomacy" and as an act of aggression towards an EU member state, there is also an overall feeling that the EU needs a more functional partnership with Turkey. There is also a feeling that Brussels may also see advantage in forging a new deal with Ankara—one that would legitimize and solidify the arrangements that were

stipulated in the Eu's offer to Turkey of a "positive agenda"—including high-level dialogue—the upgrading of the Customs Union agreement, and the renewal of the 2016 refugee deal.

Germany—now with a new government headed by a new chancellor—could use this opportunity to provide the leadership needed to mend fences with Turkey. Tackling the problems that are found in the Eastern Mediterranean would also stop the dangerous Transatlantic rift in its tracks.

Until now, the EU's engagement with the Eastern Mediterranean was overshadowed by France, Greece, and the RoC, on the one hand, and marked with an unrelenting focus on its volatile relationship with Turkey, on the other.

Indeed, more is expected now of Germany and of the country's new chancellor in foreign policy leadership, after a series of successful diplomatic interventions with Angela Merkel at the helm. For instance, during what became known as the "refugee crisis" too, Germany relied on its extensive societal, economic, and political ties with Turkey to take the lead in EU-Turkish relations and negotiate the 'refugee deal' with Ankara. And at the height of the 2020 Greece-Turkey standoff, it was German diplomacy that averted a complete breakdown of relations. It is also well-known that Athens and Berlin clashed at a EU Council meeting when Athens demanded a statement to welcome the eleventh-hour deal it had reached with Egypt, demarcating the two countries' exclusive zones. The deal was announced much to Germany's fury a day before the scheduled announcement of exploratory talks between Ankara and Athens that Berlin had brokered.

It is true that Germany's leadership in the EU is based on the constant interaction and consensus-seeking between Berlin and the other member states, France in particular. But this makes the German leadership in EU foreign and security policy a diplomatic affair, and an important counterweight to France's often belligerent and hawkish approach. More to the point, France's involvement in military exercises or more recently in exploration alongside Greece in disputed waters, as well as its push to join the East Mediterranean Gas Forum, has added to tensions at times when Berlin was engaged in talks aimed at reducing them.

For its part, Turkey also knows too that it is ultimately the EU that holds the key to unlocking the Eastern Mediterranean conundrum. Cyprus and Greece are member states, and Turkey itself is still within the EU accession framework. The EU countries have already offered Turkey a "positive agenda," and there is no reason for Brussels not to continue pressing on with a wider, regional dialogue in the Eastern Mediterranean while advancing cooperation with Turkey within that positive agenda.

Having said that, Berlin and Paris must bridge their differences and work together to advance common EU positions. In this regard, Paris would do well to compartmentalize its differences with Turkey, as the latter has done in other cases. Paris could also use its close ties with Athens and the other EMGF states to emphasize the importance of dialogue. Germany, meanwhile, should continue to use its economic and political leverage over Turkey to ensure Ankara remains committed to its de-escalatory approach, and seek ways to inject a positive dynamic to the overall EU-Turkey relationship that is sorely lacking.

To ease tensions that exist, avert a new standoff, and start a dialogue, more engagement on the part of Germany may just be what is needed.

Convening the Conference

The maritime standoff among Turkey, Greece, and Cyprus in the Eastern Mediterranean has already torn through Europe and divided NATO. Paris, for its part, has thrown its weight behind Greece and Cyprus by promoting punitive and escalatory measures toward Turkey in the Eastern Mediterranean. Germany on the other hand, together with Spain, Malta, and others continues to push for dialogue.

This is no time for Berlin to back down. In fact, to ease tensions that exist, avert a new standoff, and start a dialogue, more engagement on the part of Germany may just be what is needed. By taking a leadership role, Germany could renew efforts toward convening an Eastern Mediterranean Conference, which remains the only concrete proposal that both EU and Turkey say could reduce tensions and open a channel for dialogue.

And no matter how ambitious it sounds, if the EU (or, more precisely, its key member states) succeeds in mediating a wide-ranging deal with Turkey on the Eastern Mediterranean through the aforementioned conference, it could help reset the Eastern Mediterranean states' troubled relations with Turkey whilst also paving the way for sorting out some of the other problems the two sides currently have with each other. Such leadership would, in turn, provide an important way for the EU to flex its diplomatic muscles and significantly contribute to the EU's broader agenda for re-engagement with the United States.

At the same time, the United States too should leverage its allies on the EMGF (Egypt and Israel,

in particular) to arrive at more flexible positions towards Turkey, recognizing its legitimate rights and interests in the region. As Washington pivots to Asia, U.S. President Joe Biden may prefer not to invest too heavily in resolving the Eastern Mediterranean's maritime disputes. It is also true that relations with Turkey are at a precarious state due to its purchase of Russian S-400 missile in 2017. But Washington should nonetheless be concerned about the possible fallout from the dispute—considering its repercussions for the NATO alliance.

In this regard, American policymakers would do well to recognize that China and Russia will be eager to capitalize on any void and conflict among the allies in the Eastern Mediterranean. Those two powers are already able to maneuver well in the region, taking advantage of the increasing disorder. The hasty notion of strategic autonomy, promoted on the back of the souring of relations with Turkey, also risks turning the NATO into a bifurcated alliance. Turkey remains an important NATO ally and host to U.S. bases; pushing it more toward Russia will bear its own perils.

Now that Turkey has strengthened its position in the Eastern Mediterranean through robust countermoves, it has also adopted a tentative de-escalatory approach. It has indicated that it is open to working with the EU and NATO in Afghanistan, Iraq, Libya, Syria, and Ukraine—showing a good degree of alignment with Western interests. The very recent Turkish request to purchase a fleet of F-17 fighter jets from the United States should also be seen in this same context of reconciliation. On the Mediterranean front too, Ankara has recently reached out to Israel to normalize relations, and to Italy in seeking alternative arrangements that could benefit Turkey economically. Back-channel discussions with Egypt are also ongoing.

The U.S. and the entire EU membership should also embrace this de-escalatory approach, recognizing that a strong Greece-Turkey relationship is in the interest of the entire Transatlantic community. Convening the Eastern Mediterranean Conference at the earliest opportunity would be a good step in the direction of demonstrating that it is possible for the Transatlantic community to solve the disputes that surround the sharing of the Eastern Mediterranean's energy resources through dialogue. This would truly constitute a "win-win" situation for all parties.

A SELECTED LIST OF DISTINGUISHED AUTHORS FROM THE FIRST NINETEEN ISSUES OF HORIZONS


IAN BREMMER


GORDON BROWN


TURKI AL-FAISAL


NIALL FERGUSON


GEORGE FRIEDMAN


WOLFGANG ISCHINGER


JIN LIQUN


PARAG KHANNA


CHRISTINE LAGARDE


SERGEY LAVROV


JACOB J. LEW


JOHN J. MEARSHEIMER


THIERRY DE MONTBRIAL


DAVID MILIBAND


AMINA MOHAMMED


JOSEPH S. NYE, JR.


NGOZI OKONJO-IWEALA


NOURIEL ROUBINI


KEVIN RUDD


JEFFREY D. SACHS


FRANK-WALTER STEINMEIER


NEERA TANDEN


YANG JIECHI

You may read their articles and many more by visiting
www.cirsd.org/horizons

Minda de Gunzburg
Center for European Studies Harvard

The Minda de Gunzburg Center for European Studies at Harvard University congratulates CIRSD on its twentieth edition of *Horizons*.

In the current moment of physical separation, the dissemination of ideas is imperative for sustaining thoughtful intellectual engagement and inspiring action.

@EuropeAtHarvard