WINTER 2022 / ISSUE NO.20

$ 15.00 | € 10.00 | 1500 RSD

HORIZONS

JOURNAL OF INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

ISSN 2406-0402

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

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.

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.

> *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.*

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."

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.

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

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.

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."

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

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.

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.

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 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).

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.

> *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.*

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.

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.

> *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.*

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.