AUTUMN 2016 / ISSUE NO.8

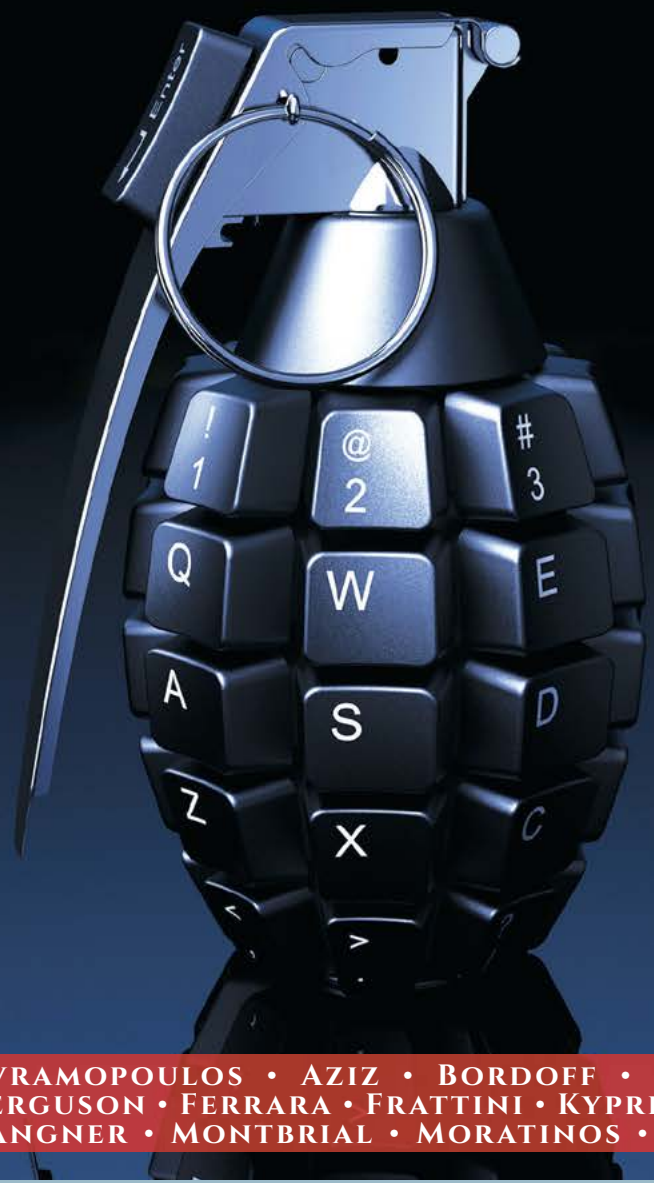
$ 12.00 | € 8.50 | 1000 RSD

HORIZONS

JOURNAL OF INTERNATIONAL RELATIONS AND SUSTAINABLE DEVELOPMENT

ISSN 2406-0402

GLOBAL SECURITY CHALLENGES



AVRAMOPOULOS • AZIZ • BORDOFF • ÇANDAR • EYAL
FERGUSON • FERRARA • FRATTINI • KYPRIANOU • LAHOUD
LANGNER • MONTBRIAL • MORATINOS • NIBLETT • SHIN

cirsd.org

CYBER POWER

AN EMERGING FACTOR IN NATIONAL AND INTERNATIONAL SECURITY

Ralph Langner

THERE is little doubt that cyber's role as a significant factor for national economies, trade, and public political debate, will only increase. The amount of time end users spend on the internet using social media, news outlets, or online shopping is only the surface of the structural change that society and the economy is undergoing—from cyber-charged consumer technology, like the so-called Internet of Things, to deep technological upheavals, such as "smart" electric grids and the Industrial Internet.

Accordingly, digital technology demands political governance. Yet, despite this need, we are witnessing political leaders' expressions of unfamiliarity with key facts and developments. They confess that the internet is "*terra incognita* for all of us"—as German Chancellor Angela Merkel said in 2013, with the "us" referring to the German political administration at large.

In this essay, I attempt to give an overview of what I consider as essential knowledge for cyber policymaking, without using much technical jargon. While there is explanatory literature available on the subject, my viewpoints may differ from mainstream discourse: I am not a scholar of international relations or political science, but rather a long-time practitioner in defending high-value targets in critical infrastructure against potential cyber-attacks.

CYBER POWER DEFINED

Cyber power is a society's organized capability to leverage digital technology for surveillance, exploitation, subversion, and coercion in international conflict. A society wielding substantial cyber power can engage in a substantial number of actions: it can economically exploit or undermine other nations; gather political and military intelligence more efficiently than pre-digital espionage; interfere

Ralph Langner *is a co-founder of The Langner Group, an international cyber defense consultancy. He gained global renown for cracking the Stuxnet malware. You may follow him on Twitter @langnergroup.*

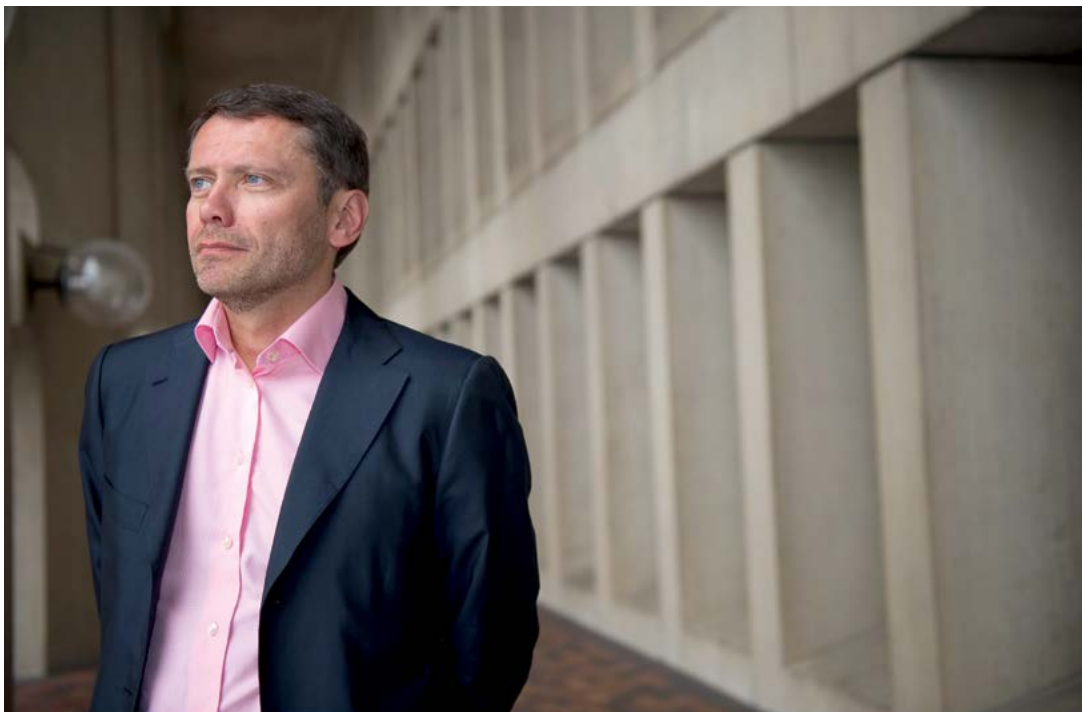


Photo: Guliver Image/Getty Images

Ralph Langner

in foreign political discourse online; degrade an adversary's warfighting capabilities; sabotage critical infrastructure and industrial mass production, and even cause mass casualties. All of this can be done through the clever application of digital technology and without necessarily deploying military forces or human spies.

Unlike traditional military domains like air or sea power, a society can jumpstart noteworthy cyber power without the corresponding capabilities in their civilian economy. This can be described as the equivalent of a country being capable of building a modern air force without maintaining a commercial civil aviation sector. Some examples include technologically underdeveloped countries like Iran, Tunisia, and North Korea—all of which maintain cyber armies. Moreover, while the cyber forces of, say, Iran or North Korea will never rival the U.S. National Security Agency, they are still capable of presenting a credible threat to the security of other nations.

The low entry barrier to the cyber club is mostly due to the poor defensive posture of the majority of relevant targets in international conflict, from the private sector to the supposedly secret systems and networks

of the military-industrial complex. Time and again, we have witnessed high-profile cyber attacks that have used anything but highly sophisticated "zero-day" attacks, yet still manage to accomplish their objectives using well-known exploits that have circulated on the internet for years. Even easier to take advantage of are security weaknesses that are deliberately designed into many digital systems that control critical infrastructure, commonly known as Industrial Control Systems; when authentication is not supported by a specific product, an attacker does not even need to crack passwords.

Cyber power is a society's organized capability to leverage digital technology for surveillance, exploitation, subversion, and coercion in international conflict.

Given the cheap entry ticket to cyber power, it is only rational that not just the great powers, but especially smaller nations, rush to develop military cyber forces. As of today, more than 100 countries are assumed to maintain cyber armies—and this is not counting digital espionage, which is a routinely used tool of traditional intelligence branches.

Cyber power can be projected by the infiltration of foreign digital systems. This requires research and some analytical process, but is not as risky, attributable, or expensive as deploying expedition forces. Getting bytes on the ground may be accomplished via the internet—commonly referred to as hacking—or by having unwitting or collaborating insiders to insert a weaponized USB stick into the right computer.

Such infiltration needs to be accomplished well in advance of an actual cyber strike. For all but the worst defended targets, a sophisticated cyber-attack cannot be launched within hours, or even days, against targets that have not already been infiltrated.

In technical terms, the organized capability required to sustainably project cyber power is extensive. This should include an infrastructure with command-and-control servers; a workforce of software developers capable of developing exploits and destructive code sequences; subject matter experts who know what to search for or which systems and data to manipulate; and big data analytics to process what can amount to terabytes of exfiltrated data.

Critical Infrastructure at Risk

The most widely discussed cyber risk to national and international security is the impairment of

critical infrastructure, such as a nationwide blackout of the electric grid. As it happens, the energy sector at large—including the generation and transport of electric energy, as well as oil and natural gas—is hit almost constantly by cyber intruders. Other logical targets include water supply and the financial industry.

At present, a nationwide blackout of the electric grid of a large economy, such as the United States, would require substantial cyber capabilities that may currently be at the disposal of very few first-tier cyber powers, such as Russia and China. Thankfully, however, there seems to be no good reason for them to proceed with such a course of action, at least not in peacetime.

The low entry barrier to the cyber club is mostly due to the poor defensive posture of the majority of relevant targets in international conflict, from the private sector to the supposedly secret systems and networks of the military-industrial complex.

Second- and third-tier actors, such as Iran or North Korea, or even non-state actors, presently do not have the capability to cause large-scale blackouts. Nevertheless, they may be able to pull off small-scale attacks, such as taking down regional electricity grids or water supply utilities. Depending on the target—examples worth discussing include Washington, Paris, or London—such attacks may still have a high impact.

An emerging target set is also the industrial mass production sector—or critical manufacturing—with its present rush to digital hyper-connectivity. Several nations are already pursuing major programs to propel the digitization of industrial production, termed the Industrial Internet in the United States, or Industrie 4.0 in Germany. Similar programs have been launched in China and Japan.

While at this time there is no proof of the alleged benefits of a hyper-connected industrial infrastructure, proponents claim that the results will be as disruptive as the introduction of the steam engine or assembly line.

If such perceived benefits lead to the widespread adoptions of digital controls, they will become a prime target for offensive cyber strategy, including both industrial espionage and digital coercion. At this time, there is very little indication as to how the Industrial Internet will be safeguarded against these kinds of attacks.

We have not yet seen a substantial cyber attack against a nation's critical infrastructure that

has seriously affected national security. There are, however, precedents on record. A recent example is the cyber attack against parts of the Ukrainian power distribution system just before Christmas 2015, which left some 200,000 households in the dark for several hours. While first-hand forensic evidence is not publicly available, what we do know about this attack indicates that an utterly negligent configuration at the Ukrainian source played a major role; deliberate configuration decisions that grossly traded security for convenience were exploited.

Given the cheap entry ticket to cyber power, it is only rational that not just the great powers, but especially smaller nations, rush to develop military cyber forces.

Other examples are widely recognized. Cyber attacks against America's financial sector, which started in 2013, are usually regarded as having been provoked by Stuxnet and are attributed to Iran as a means of revenge. While monetary damage was caused, the impact on the economy and American national security was minimal. A year earlier, 30,000 office computers at Saudi Aramco, Saudi Arabia's national oil and gas company, were rendered useless by a cyber attack that is also assumed to be part of Iran's retaliation for Stuxnet. If we go further back in history, the 2007 cyber attacks against Estonia had all the characteristics of yet another tit-for-tat message exchange; an obvious reaction to political events that a potent neighbor (Russia) did not appreciate.

Tactical Military Objective

The common thread in all of the previously referenced attacks is a highly visible but non-critical—i.e. symbolic—reaction to an initiating event that may or may not be digital. One can only assume that we will see similar attacks in the future, with Russia, Iran, and North Korea among the usual suspects.

But there are other kinds of cyber attacks, such as when an attack serves a direct tactical purpose within a smoldering international conflict. The poster child of this category is the Stuxnet attack against the Iranian nuclear program.

From the forensic analysis that I conducted, it is clear that the attackers had the capability to take down major components of the Iranian energy infrastructure had they chosen to do so. Instead, they opted to covertly throw sand in the gears of Iran's uranium enrichment program and "make it look like an accident"—to quote a popular line from the movies. One side effect of the low-yield strategy was that it remained unclear whether this could qualify as a

military use of force, thus barring the legal framework from classifying it as an act of war—something that even Iran did not claim in the aftermath of the attack.

Stuxnet had a clear tactical purpose in delaying the Iranian nuclear program, while at the same time making Iran believe that all problems with its fragile centrifuges were rooted in its own technical incompetence. In any case, Stuxnet was very different from merely sending a message, if only because it was intentionally disguised and was surprisingly successful in remaining hidden for as long as three years (from 2007 to 2010).

For all but the worst defended targets, a sophisticated cyber-attack cannot be launched within hours, or even days, against targets that have not already been infiltrated.

Another high-profile case on the record is the 2008 wave of cyber attacks against Georgia, during which more than 50 communications, finance, and government websites were attacked. Three weeks after the attacks started, Russian forces entered the country. In some instances, local government websites were under distributed denial-of-service attacks in synchronization with air strikes.

While there is no definitive evidence available on who was behind the sustained cyber attacks, the events are considered as the first case in history of a blended cyber and kinetic attack. We have little empirical evidence to prove it, but it should be taken for granted that digital military systems, from surveillance and warship propulsion to steering and weapon control systems, are all prime targets of cyber intruders and their attempts to degrade said systems' performance in combat. One sparsely documented incident that illustrates this point is how Syrian air defense systems were compromised during the Israeli air strike against an alleged hidden nuclear facility in 2007, known as Operation Orchard.

This class of cyber attack can be viewed as highly ambitious, since attack execution must be tightly synchronized with kinetic action—something that is particularly challenging without the luxury of effective online command and control. At this time, the United States, Israel, and Russia apparently have such tactical military cyber capabilities. The same can be assumed about China, the United Kingdom, and France.

CYBER DEATH & DESTRUCTION

All the talk about a potential "Cyber 9/11" ignores the fact that it is very difficult to kill the same magnitude of people who died in the Twin

Towers with bits and bytes. Having said that, it is absolutely possible to kill, and thereby terrorize, a large population.

The most effective way to achieve this would be to release hazardous material with relevant targets in the chemical and nuclear industry. These are often much less protected against cyber attacks than would be expected by the general public, the media, or political leaders. While there may be little probability that a nation state would actually pursue this avenue, it is worth underscoring the obvious fact that terrorists are not signatories to the Geneva Convention and might not be deterred by the prospect of overwhelming retaliation. Even if one bets chemical and nuclear safety on the (plausible) idea that present-day terrorists do not have the capability or resolve to engage in highly sophisticated and devastating cyber attacks, it should be understood that upgrading relevant systems toward achieving high digital resilience often takes between five and 10 years.

The most widely discussed cyber risk to national and international security is the impairment of critical infrastructure, such as a nationwide blackout of the electric grid.

We have no guarantee that, in the meantime, terrorists will stick to their preference of using suicide bombers as the weapon of choice.

Chemical plants are of particular importance because of their sheer numbers. In the United States alone, for example, approximately 4,000 plants are designated as high-risk. These plants are subject to terrorist threats due to their capacity to store or process hazardous material in high quantities. One could imagine a scenario in which a widespread release of toxic gas could—as it did in the 1984 Bhopal incident—leave several thousand dead and hundreds of thousands injured.

Technically, an explosion or other similar event that causes injuries and death, such as opening the wrong valves at the wrong time, can almost always be seen as a failure of safety systems. Safety in this case—i.e. the technology and procedures that assure that plant malfunction cannot result in casualties—is a science in its own right.

Unfortunately, the engineering behind safety systems does not factor in malicious manipulation. Safety deals with random component failure and adverse events, such as earthquakes, all of which can be assigned statistical probabilities. Not so for malice: what works well against nature and bad

luck achieves little against competent cyber attackers.

Efforts to marry safety with security are still in their infancy and can prove exceptionally difficult to implement—even more so when digital complexity enters the picture. As the U.S. Nuclear Energy Institute (NEI)—which is not biased towards an anti-nuclear agenda—noted in 2013:

> When the methodology to address cyber security controls was developed in the template for the cyber security plan, the industry believed there would be small handfuls of digital assets (CDAs) that would require a cyber security assessment. However, NEI understands that plants, including those with no digital safety-related systems, have identified many hundreds if not thousands of CDAs.

Upgrading relevant systems toward achieving high digital resilience often takes between five and 10 years.

The other uncomforting truth in this statement is that even if a completely analog (and thus unhackable) safety system is used, immunity against cyber attacks is not guaranteed. As others and I in the nuclear safety realm have argued, in a highly digitized environment there are possibilities to create process conditions outside of the design limits of the safety system, thereby potentially subverting even fully functional safety logic.

Rational Cyber Conflict Strategy

The number of high-profile destructive cyber attacks against critical infrastructure on record is low. It would be regrettable if this led non-technical pundits to assume that such attacks would be too difficult for the usual suspects to execute. On the contrary, technical analysis suggests otherwise.

Looking at the big picture of sophisticated cyber intrusions, it is apparent that various actors pursue the doctrine that global cyberspace is an open range for infiltration. With this in mind, the intent is to keep one's powder dry, rather than taking the first cyber shot when one is presented with such an opportunity. Here are some illustrative examples.

In 2012, it was discovered that Telvent, a Canadian manufacturer of software for the Smart Grid and for oil and gas pipeline operators, was breached. In North and Latin America, the company's software is used to control more than 60 percent of the movement of hydrocarbons. The breach was particularly sensitive, because it affected the company's remote access to hundreds of international customers in the energy sector. It could have ultimately given the attacker the capability

to interfere with the energy supply in multiple countries.

The Telvent breach, though, was small potatoes compared to modern-day attack campaigns, in which the target is not a specific company but rather hundreds or thousands of organizations in one or more industry verticals—with a main thrust against the energy sector. Iconic examples are the (distinct) campaigns dubbed Energetic Bear and Black Energy by various computer security companies and the U.S. government.

In a highly digitized environment there are possibilities to create process conditions outside of the design limits of the safety system, thereby potentially subverting even fully functional safety logic.

Energetic Bear and Black Energy do not utilize just one isolated piece of malware, but rather a whole malware warehouse, with the attackers being able to pick their exploit of choice for the cyber mission of the day. An attack infrastructure employing several hundred command-and-control servers, as well as big data analytics that process terabytes of exfiltrated data, suggests that the forces behind these campaigns have large plans. Most disconcerting about Energetic Bear and Black Energy is the fact that they contain exploit modules which exfiltrate data without value for industrial espionage, whilst being useful for the preparation of destructive attacks.

Large-scale campaigns like these can be viewed as the most rational emanation of modern cyber strategy. In the tradition of Thomas Schelling, we observe that the exploitation of potential force, or the threat of force, can be as powerful as, or even more than, the actual application of force.

A rational cyber power will go for large-scale infiltration of its adversaries' critical infrastructure—earlier described as the projection of cyber power—but will not necessarily execute their destructive capabilities in a high-profile cyber strike, which would almost certainly trigger repercussions. But why deal with such escalatory risk when infiltrations are regarded as the new normal and are not really sanctioned. Cyber intruders need not worry if they are detected or not; just the opposite, in fact, as it helps them gain notoriety and adds to the deterrent.

A case in point, reported earlier this year, is how a small floodgate (misinterpreted by the media as a dam) in New York State was compromised by a group of Iranian hackers. When the culprits were ultimately indicted, Iran must have

viewed it as a price worth paying in exchange for having prime media coverage from the *New York Times* and *Time Magazine* speculate about the Islamic Republic's capabilities of crippling critical infrastructure in the United States.

For a deterrent to be useful, the counterpart needs to be convinced, or at least seriously consider, that the adversary in question actually has both the capability and willingness to act upon it. The media got Iran a long way towards that end.

The availability and use of cyber weapons may escalate a minor conflict into a major crisis, and ultimately even kinetic war.

With cyber intruders of diverse backgrounds busily infiltrating everything from military networks to the most obvious honeypot (a fake digital system to attract attackers and study their behavior), it is predictable that cyber intrusions of critical infrastructure will continue towards some form of Nash equilibrium.

The main risk for the attacked nation is that creeping infiltration can reach a quantum leap, at which point quantity turns into quality. If the victim does not say "enough is enough" (while still capable of doing so), one might find oneself in a position that resembles the metaphor of slowly boiling a frog—the frog will become incapable of jumping out of the simmering water.

Impacts on International Stability

Does the emerging role of cyber power in international conflict result in more or less international stability? As long as the major thrust goes to offense, I remain in the 'less-stability' camp. The availability and use of cyber weapons may escalate a minor conflict into a major crisis, and ultimately even kinetic war.

Two major factors need to be considered in this context. First, the advent of non-state actors that are not bound to international norms and do not care about escalation, or maybe even intend on provoking escalation. Second, specific cyber attack scenarios may leave the victim with few options other than a kinetic response. Imagine a scenario in the context of the cyber attack against Saudi Aramco: let us assume that instead of destroying the data of 30,000 office computers at the oil giant, the attackers had managed—either on purpose or by accident—to shut down operations at the Ra's Tanura oil terminal for weeks. It is not unrealistic to assume that, in such a case, Saudi Arabia would be left with little choice other than a kinetic counterstrike.

Another group of concerning escalatory scenarios involves the digital degradation of an adversary's warfighting

capability. Former U.S. Secretary of the Navy Richard Danzig has elaborated on the prototypical scenario in which a nuclear power would compromise another's nuclear command and control infrastructure, thereby undermining its second strike capability. Ultimately, as Danzig points out, the victim might feel compelled to execute a first strike. As this example illustrates, cyber may affect the nuclear strategy of mutually assured destruction, a doctrine that has brought stability for decades.

What we are currently witnessing can be characterized as the teen years of cyber conflict, dominated by immature, rude, aggressive, and experimental behavior. Today, cyber power and its applications are still largely determined by offensive capabilities and those actors that are exploring, testing, and using them. It is predictable that the balance of power in the future will be shaped by passive defense, which may lead back to more stability. There is a technical reason for this: while there is no bunker strong enough to shield against a nuclear blast, cyber weapons are only as effective as the vulnerabilities they exploit. Zero-day exploits and other aggressive digital tactics do not exist in their own right, but only to the extent to which the target design features vulnerabilities.

What we are currently witnessing can be characterized as the teen years of cyber conflict, dominated by immature, rude, aggressive, and experimental behavior.

In cyberspace, much more than in kinetic warfare, Sun Tzu's axiom applies: the opportunity to defeat the enemy is provided by the enemy himself. Critical infrastructure and the military can, in fact, be reasonably secured against cyber attacks—at least in the present and near future—from second- and third-tier cyber powers and non-state actors.

Effective reductions of the digital attack surface will directly degrade the adversary's cyber power, up to the point where it becomes too costly to threaten or attack with a reasonable chance for success. In other words, technologically advanced nations have the option to outspend their adversaries on cyber defense.

Core Issues for Policymaking

Unfortunately, technologists will not be able to "solve" cyber insecurity, since it is inherent in digital technology itself. An insecure system or procedure is inherently more flexible, more convenient, and less costly than a secure one. Security typically comes with a measure of inconvenience, inflexibility, or extra cost in acquisition, usage, and maintenance.

The trade-offs required to move toward better security are essentially

decisions that are being made—consciously or as concluding behavior—by private end users, as well as by companies and governments.

I would like to conclude this essay by discussing three of the most fundamental questions in this decisionmaking process that need to be addressed in political discourse.

The first question is: *What is cyber security worth?* Security is not free. More cyber security will never make a quarterly balance sheet look better, nor will it ever produce a surplus budget. On a societal scale, cyber security should be viewed as a public good, analogous to environmental protection and clean energy. The cost of making a society reasonably resistant to cyber attacks from anyone beyond first-tier actors may equal that of existing programs to substitute fossil fuel. Such a cost is also not, alas, a recipe for economic growth or enhanced competitiveness in global markets.

There is little to be said against a society which consciously and deliberately decides against paying such a cost so long as it is at peace with betting its national security and prosperity on the hope of reasonable behavior of various adversaries, many of whom who are believed to be restrained by deterrence. At the same time, it can stop promoting governmental baby steps towards better cyber security, often sold as robust strategic plans.

Unfortunately, technologists will not be able to "solve" cyber insecurity, since it is inherent in digital technology itself.

The second question to ask is: *What is an appropriate balance of offensive and defensive cyber efforts?* Today, governments are the biggest customers of exploits. Governments fuel the cyber exploit industry, and every government that hosts a military cyber branch possesses a stash of zero-day vulnerabilities—and commands exploits that rock.

Despite all Sunday talk on the importance of information sharing, the defensive branches of these same governments are sometimes left in the dark when it comes to these vulnerabilities—all to avoid spoiling valuable equity.

One would also like to see public discussion and the forming of opinions on whether it would be wise to develop more offensive cyber capabilities against which a society would be able to defend itself, and on appropriate budget balancing for defensive and offensive cyber programs—the latter of which is usually not fully disclosed.

The third and final question to pose is: *What is the red line for cyber intruders, and how can it be enforced?*

One can predict that large-scale cyber intrusions of critical infrastructure will continue to the point where they pose a threat to national security and political willpower—simply put: to a state's sovereignty.

On a societal scale, cyber security should be viewed as a public good, analogous to environmental protection and clean energy.

This development must be prompted by political decisionmakers, who should define a clear and robust red line. International acknowledgement of such a red line would be encouraged by reciprocity in the form of international treaties, in which parties should commit not to cross the proportional red lines of others.

www.cirsd.org/horizons

A SELECTED LIST OF DISTINGUISHED AUTHORS FROM THE FIRST SEVEN ISSUES OF HORIZONS


JACQUES ATTALI


CARL BILDT


IAN BREMMER


GORDON BROWN


HELEN CLARK


LAURENT FABIUS


NABIL FAHMY


TURKI AL-FAISAL


PAUL R. GALLAGHER


WOLFGANG ISCHINGER


JEAN-CLAUDE JUNCKER


MUHTAR KENT


CHRISTINE LAGARDE


SERGEY LAVROV


DAVID MILIBAND


THIERRY DE MONTBRIAL


JOSEPH S. NYE, JR.


NGOZI OKONJO-IWEALA


ITAMAR RABINOVICH


KEVIN RUDD


JEFFREY D. SACHS


JAMES STAVRIDIS


FRANK-WALTER STEINMEIER


YANG JIECHI

cirsd

You may read their articles and many more by visiting
www.cirsd.org/horizons