Cyberstability Paper Series

New Conditions and Constellations in Cyber

Closing the Gap: Expanding Cyber Deterrence

Michael Daniel
CEO of the Cyber Threat Alliance; Former Cybersecurity Coordinator, US National Security Council

July 2021

Cyberstability Paper Series
New Conditions and Constellations in Cyber

Closing the Gap: Expanding Cyber Deterrence

Michael Daniel | CEO of the Cyber Threat Alliance; Former Cybersecurity Coordinator, US National Security Council

July 2021

While cyber deterrence is a logical goal, it often seems rather elusive. Certainly, the volume, intensity, and impact of malicious cyber activity have grown substantially over the last few years, leading some thinkers and practitioners to argue that deterrence will not work in cyberspace.[1] The public evidence points in the other direction, however: deterrence can and does work in cyberspace. Nation-states could undertake regular, sustained, destructive actions in and through cyberspace if they wished, but they do not, because deterrence affects their decision calculus. Instead of not functioning at all, cyber deterrence is insufficient in its current form.

First, a gap exists between activities that cannot be realistically deterred (such as espionage) and those that are already deterred (such as nation-states undertaking widespread, frequent, destructive cyberattacks against critical infrastructure assets outside of armed conflict). Yet, activity that falls within this gap causes measurable harm, violates internationally agreed upon norms or "rules of the road" of cyber behavior, and is potentially destabilizing to international peace. Second, malicious cyber activity is often cumulative in its effects, yet individually not all that harmful. Any single theft of intellectual property or business disruption might not rise to the level of a national security threat, but, taken collectively, these activities become significant problems. As a result, cumulative, counter-normative, and consistent malicious cyber activity falling within the deterrence gap threatens many nations, damaging their national security, reducing economic prosperity, and harming public health and safety. Given the physical characteristics of cyberspace and the multiplicity of malicious actors with different motivations, a single policy approach, such as Mutually Assured Destruction, cannot shrink this deterrence gap, nor can it reduce the volume, intensity, and impact of malicious activity that might occur in a smaller gap. Rather, expanding cyber deterrence requires

Michael Daniel is the President and CEO of the Cyber Threat Alliance. From June 2012 to January 2017, he served as Special Assistant to President Obama and as Cybersecurity Coordinator on the US National Security Council.

changing our mindset about how cyberspace works and creating a set of interlocking policies with different aspects, depending on the malicious actions being deterred. Implementing such expanded deterrence policies could generate substantial benefits for the digital ecosystem.

For many people, the term "deterrence" conjures up images of the Cold War and nuclear deterrence. Nuclear weapons are so destructive, so terrifying, that the primary goal for nuclear deterrence is zero use. The United States and its allies achieved that goal during the Cold War, and we have sustained that success so far in the 21st century. In fact, the resulting norm against nuclear weapon use is so deep-rooted that even non-state actors have largely shunned such capabilities, despite fears that the weapons would appeal to them. The success of nuclear deterrence means that all other deterrence efforts tend to be measured against it.

However, nuclear deterrence is not the right benchmark for cyber deterrence. First and foremost, zero use is not a realistic goal for cyber deterrence policies. The nature of cyber activities differs substantially from that of nuclear weapons; cyber effects are usually scalable, reversable, and vary widely in impact. Even nations that feel deeply about it cannot credibly threaten to conduct military strikes for low-level cyber espionage or extortion, nor does international law permit such disproportional responses. Further, the ability to confuse attribution, obfuscate activity, create ambiguity, and operate in an undetected manner makes complete deterrence infeasible. Finally, the motivations of cyber actors can differ substantially. Criminals are in it for the money, while nation-states are pursing national security goals. What deters money seekers is different from what deters security-minded government agencies.

As a result, even expanded cyber deterrence policies are not going to stop all malicious cyber activity. Such policies will not stop cyber-enabled espionage. They will not prevent nations from employing offensive cyber capabilities as part of their national security tool set, nor will they eliminate cybercrime from the Internet. A certain level of malicious cyber activity will be endemic to cyberspace, just like a certain level of malicious activity is endemic to the physical world. We can aim for world without the use of nuclear weapons; the same is not true for malicious cyber activity.

On the flip side, arguing that "deterrence" as a concept does not work at all in cyberspace ignores what already does not happen. Nations—such as the United States, the United Kingdom, Israel, China, Russia, and Iran—could use their offensive cyber capabilities to cause widespread disruption, even physical destruction, on a regular basis. For example, as part of its efforts to disrupt the Islamic state, the United States conducted cyber operations to disrupt their communications;[2] the United States could regularly undertake such activities against foreign governments, if it so chose. The Russian government turned the power off in Ukraine in December 2015 and December 2016;[3] they could choose to take such actions against power plants in other countries on a regular basis. If a criminal ransomware attack can shut down a manufacturer such as Norsk Hydro[4] or a critical infrastructure such as the Colonial Pipeline,[5] nation-states could use those capabilities much more often than they do. Yet, they do not.

Some restraint stems from economic self-interest, because most nations benefit from the economic activity that occurs in cyberspace. Another restraint comes from practicality, as cyber operations are more difficult to undertake than Hollywood movies portray. However, since nation-states sometimes use these capabilities, economic self-interest and technical difficulty alone are insufficient to explain the lack of offensive cyber activity. These nations choose not to use their offensive cyber capabilities in this manner partially because deterrence works—using such capabilities profligately would invite retaliation through a variety of means, including physical force. To explain the

relative paucity of disruptive or destructive nation-state cyberattacks, deterrence must factor into the explanation. Even cybercriminals try to maintain a degree of anonymity and avoid traveling to Western nations, so some minimal level of deterrence operates even against cybercrime.

Although some activities cannot be realistically deterred (such as espionage) and others are already deterred (e.g., nation-states undertaking widespread, frequent, destructive cyberattacks against critical infrastructure assets outside of armed conflict), a range of damaging malicious cyber activities falls in between these two types. Some nation-states and many criminal groups are exploiting this gap. These actors use cyber capabilities to cause physical disruption and harm, but not quite enough harm in any single instance that the United States or other countries have used military force to stop it. The cumulative nature of malicious cyber activity compounds the problems from the deterrence gap. Seen as individual actions, certain activity may seem to fall below the threshold of deterrability, but, when looked at in aggregate, the effects can be enormous. Ransomware is a good example. Although most individual ransomware attacks fall below the use of force as defined in international law, collectively ransomware attacks threaten our national security, economic prosperity, and public health and safety. Ransomware's aggregate burden is not sustainable over the long term at current levels.

The problem for cyber deterrence is not whether it works at all, but whether it can be expanded to work against a broader set of cyber activities and how to identify the activities that we want to deter.

Thus, the problem for cyber deterrence is not whether it works at all, but whether it can be expanded to work against a broader set of cyber activities and how to identify the activities that we want to deter. At present, the deterrence gap is big enough that activity falling within the gap is causing long-term harm to national security, economic prosperity, and public health and safety in both the digital and physical worlds. Therefore, the United States and like-minded nations should seek to implement a set of expanded cyber deterrence policies that shrink the size of the deterrence gap, reduce the volume, intensity, and impact of malicious cyber activity that falls within this gap, and reinforce agreed upon norms of behavior in cyberspace.

The United States and other nations have laid a good foundation for cyber deterrence policies through efforts to establish norms of acceptable behavior in cyberspace. Since 2013, with the agreement at the United Nations that international law applies in cyberspace and that states should adhere to eleven specified norms, international debate has focused on identifying specific actions that represent violations of those norms and how to enforce them.[6] For the United States, its 2018 National Cyber Strategy articulated two concepts of deterrence, denial and cost imposition; the second concept is the method for holding norm violators accountable.[7] This strategy provides a good scaffolding for deterrence policy. However, to expand cyber deterrence to better enforce the agreed upon cyber norms, all states that are serious in upholding these norms need not only to build out those concepts, but also—collectively—to think differently about cyber deterrence. Accordingly, the first step in expanding our deterrence efforts is to adopt new mental models.

Not surprisingly, the mental models most policy makers have for cyberspace are based on the physical world; after all, that world is what we experience. However, those mental models do not work well for cyberspace, because the physics and geometry of near light-speed, nodal networks and devices differ significantly from that of the continuous physical world. Any expanded cyber deterrence policies must adapt to these physical differences.

First, no locations exist in cyberspace outside the nodes; information packets can only move from one node to the next along predetermined paths. Packets cannot stop somewhere in the middle. Second, the structure of cyberspace means that concepts of "near" and "far" differ from those of the real world. Such concepts are defined by the route or path between nodes in the network, not by their physical location on earth. Thus, "proximity" also has a different meaning, depending on the path required to move between nodes. Third, fast and slow also have different meanings; "slow" on the Internet still generally means a vastly shorter time scale than in the physical world. Fourth, cyberspace borders are very different from physical borders. Contrary to the first three, this aspect of cyberspace geometry gets a lot of attention, the most frequently used adjective being "borderless." However, conventional wisdom gets this aspect wrong. Cyberspace is not, in fact, borderless. It has a plethora of borders, with every router, firewall, and network switch creating a boundary. The issue is not the lack of borders, but the fact that cyber borders do not align with the physical world's borders and boundaries. Further, cyber borders follow their own logic and rules, which do not necessarily comport with the nation-state political structures.

As an example of how these physical factors come together to render traditional policy approaches ineffective, take the idea of border control. In the physical world, national governments control (or try to control) the flow of people and goods into and out of their territories for many reasons, including safety and security. However, when governments try to provide "cyberspace border security" in a similar fashion, it usually does not work very well. Even China, with its Great Firewall, struggles with controlling information while still allowing the Internet to perform its economic functions. The reason for these failures flows directly from the physical structure of cyberspace. Since nodes have many connections and many paths for information to take, finding, designating, and controlling a consistent "border" is virtually impossible. A nation's cyberspace does not have a geometric shape with a defined edge and a large interior; it is a lattice of points or nodes, with the points connected to huge numbers of other points through an incomprehensibly complex network of paths. "Interior" is a meaningless concept.

At the same time, cyberspace is not entirely divorced from the physical world, operating on some separate ethereal plane. Although people often act as if cyberspace constitutes a separate reality, all the computers, routers, switches, servers, and Internet-of-Things devices exist someplace on the planet, almost always in some country's territory. As a result, while the "geography" of cyberspace differs from that of the physical world, it is not entirely separate from it either.

Once mental models change to account for the different physical characteristics of cyberspace, the second step is to apply the new models to traditional deterrence approaches to see what factors need to be accounted for. Conducting such an analysis reveals at least three factors that effective cyber deterrence policies must incorporate: the need to involve non-governmental actors, the overlapping combination of malicious cyberspace actors and their motivations, and the necessity of action.

In traditional deterrence models, governments are the only actors. Among other factors, such as technical capability, the nature of cyberspace borders requires us to expand our deterrence policies to encompass additional actors, including the private sector, non-profits, and individual citizens. If no "interior" exists in cyberspace, then every person, company, organization, and government occupies some portion of a cyber border. In turn, if every organization inhabits a cyber border, then governments cannot provide cyber "border security" on their own. Further, non-state actors dominate the cyberspace ecosystem, and the Internet itself is managed through a multistakeholder model. As a result, if we want cyber deterrence policies to expand into the gap, those policies

must involve many more players than just national governments. They must incorporate the private sector, cybersecurity providers, cloud service providers, telecommunication companies, international organizations, non-profits, civil society, and critical infrastructure owners and operators. Thus, the level of coordination and organization required for effective cyber deterrence policies is much higher than in traditional deterrence efforts. Getting all those divergent actors aligned with respect to goals and activities requires more time, effort, and energy than do traditional deterrence initiatives. The work of aligning these disparate groups' activities can be considered "operational collaboration."[8] Since the government cannot compel collaboration (at least in the United States and most like-minded countries), such operational collaboration depends on nonstate actors' willing participation. Since we have not fully developed this concept of operational collaboration sufficiently to put it into practice, our previous efforts at deterrence have fallen short.

The second factor stems from the overlapping and sometimes ambiguous nature of the targets of deterrence. Traditional military or nuclear deterrence seeks to dissuade other national governments from undertaking certain military actions. It also typically focuses on an effectively small number of people within those governments. Traditional criminal deterrence is most frequently domestically focused, aimed at actors that are exclusively criminals, and spread broadly across a population. For cyber deterrence, the situation is more complex. The line between nation-state and criminal actors has become very blurred in cyberspace, whether due to the use of criminal groups as proxies (in the case of Russia) or because the government is carrying out criminal activities to circumvent international economic sanctions (in the case of North Korea). As a result, the elements related to national governments and criminals are intermixed. At the same time, though, nation-states and cybercriminals undertake malicious cyber activity for fundamentally different reasons.

Cyber deterrence policy must deal with these different motivations simultaneously. Yet, deterring someone who is seeking money is very different than deterring someone who is personally committed to advancing a cause. Actions that choke off financial flows might deter a money-seeking cybercriminal, but will not dissuade a hacktivist. Cybercriminals spend a very limited amount time or resources trying to access any given target's network. If it proves too difficult or time-consuming, they move on to other, easier-to-access victims. Accordingly, deterrence by denial often proves highly effective against cybercriminals. A nation-state, however, can be much more patient, biding its time, and expending many more resources to access a given target if they need to access that target to advance their national-security goals. Given the intertwined nature of malicious cyber actors, expanded cyber deterrence must combine policy components from military and criminal deterrence with approaches that are aimed at deterring different motivations, depending on the specific situation.

To date, the United States and its allies have not clearly tied deterrence efforts to behavioral benchmarks.

Based on this logic, the United States and those states interested in upholding the agreed norms should broaden the variety of tools used to impose different kinds of costs on the adversaries. Focusing on only one kind of cost imposition, such as an overwhelming military response or a technical cyber response, will not credibly deter as broad an array of malicious cyber actors as needed. Interlocking, multi-faceted cyber policies will have many different cost imposition elements, each aimed at a different type of malicious behavior.

Finally, cyber deterrence requires action. Nuclear deterrence relied on the threat of action, but it did not require demonstrations in the physical world to be credible. Since the potential damage from

nuclear weapons was so vast and irreversible, the threat of credible retaliation was sufficient. In fact, with zero use as the goal, the less action and the less direct confrontation, the better, as far as traditional deterrence initiatives were concerned. Nuclear weapons use was and remains binary—either they are used or not. They only result in permanent destruction and any individual weapon cannot be scaled up or down in destructiveness.

This situation is reversed for cyber deterrence. Malicious cyber action is not binary; it is often reversible, and frequently scalable, with a wide array of consequences. As a result, the mere threat of action is not sufficient to expand deterrence into the gap. Thus, enhanced cyber deterrence policies will involve action and retaliation. Such actions do not have to involve the use of military force or even military components at all, although they can. Diplomatic, law enforcement, technical counter-cyber operations, and economic penalties should also form part of that array.

With a revised mental model in place and key policy factors incorporated, the third step in expanding cyber deterrence is identifying policy design differences from traditional or current deterrence efforts. Specifically, expanded cyber deterrence policies should differ in five ways: clearly defining the new activity to be deterred, making use of comparative advantage, linking cyber issues with non-cyber issues explicitly, encompassing more than technical cyber actions, and involving active disruption.

While some ambiguity can be helpful in deterrence, too much ambiguity reduces its utility. To date, the United States and its allies have not clearly tied deterrence efforts to behavioral benchmarks. Such benchmarks would not constitute redlines (as in, if you do x, we will do y), but rather an articulation of what malicious cyber activities the United States and its allies seeks to deter beyond what is already deterred. Thus, the first design difference would be to tie expanded deterrence policies to specific behaviors. Already agreed upon international norms of behavior, such as the eleven United Nations norms or those proposed by the Global Commission on the Stability of Cyberspace, provide a tailor-made set of behaviors to incorporate into an expanded deterrence policy design.[9] Reducing ambiguity in behavior that the United States and its allies want to deter does not require committing to a specific action in response to such behavior, but effective deterrence does require a consistent overall response to such activities.

The second design difference lies in identifying an organizing principle for the effort. Since expanded cyber deterrence policies will rely on operational collaboration among a broader array of actors than will traditional deterrence activities, the challenge becomes one of building, organizing, aligning, and sustaining that collaboration. Trust is an oft-discussed ingredient of such collaborative efforts, and it is extremely important. However, a second, less examined enabling principle should be comparative advantage. Specially, cyber deterrence efforts should explicitly consider which private sector or non-profit organizations have the comparative advantage in a given task or function, and governments should closely examine where their comparative advantage lies.

Cybersecurity vendors can bring their technical understanding of how networks and devices function to shape operations, and their intelligence to help identify targets. Internet Service Providers, Cloud Service Providers, and Hosting Providers can focus on disrupting the adversary's technical infrastructure. Civil society and non-profit information sharing and analysis organizations can play connective roles, bringing together the disparate players and ensuring a broader picture of what is occurring. Governments should focus on adding context derived from intelligence and taking direct action against malicious actors. By leveraging different organizations' comparative advantages, a wider approach to cyber deterrence would have a multiplier effect, where the sum is

much greater than the individual parts. For governments, a significant challenge is engaging these nonstate actors in a way that does not treat them as subordinates, but as partners. Fortunately, many organizations already are convinced of the need for concerted international and multistakeholder actions to uphold norms of good behavior in cyberspace, and they are waiting for an appropriate engagement forum to emerge. The recently concluded first round of the United Nations First Open-Ended Working Group (OEWG) on the challenges of ICT in the context of international security demonstrated how important it is to reach out to nonstate actors.

Since the impact of malicious cyber activity is not constrained to cyberspace, efforts to deter such activity should not be confined to cyberspace either. Thus, cyber deterrence policies should explicitly link cyber issues, such as harboring cyber criminals, with non-cyber issues that the target nation cares about. For example, if Nation A wants support for a resolution on topic "x" at the United Nations and that nation is well-known for harboring cyber criminals, then other nations should require a decrease in malicious cyber activity emanating from Nation A's territory. Such linkages would be consistent with the international law principle of effective control; under this concept, governments are obliged to address criminal activity that emanates from their territories. The Obama Administration learned a similar lesson in linking cyberspace to the physical world when dealing with China's theft of intellectual property; only after the United States was willing to connect that issue with other issues in the relationship, and raise it continually through every channel possible, did China formally agree to limit such activities.[10] Linking cyber deterrence to broader geo-political relationships and actions will increase the ability to shrink the gap and reduce activity.

Effective cyber deterrence requires integrating non-cyber tools, such as diplomacy, economic sanctions, financial system constraints, civil legal processes, law enforcement action, and even military action.

As many cyber policy experts have noted, malicious cyber activity should not be met only with cyber-based responses. This aspect forms the fourth design difference from traditional nuclear deterrence. Effective cyber deterrence requires integrating non-cyber tools, such as diplomacy, economic sanctions, financial system constraints, civil legal processes, law enforcement action, and even military action. Technical cyber actions will certainly be a part of the tool set, but will only form a small part of it. Thus, cyber deterrence policies will employ a wide range of tools, selecting the tools that will have the greatest effect on the intended target. Since cybercriminals are motivated primarily by money, focusing on bringing the cryptocurrency exchanges into compliance with global financial rules could be a very effective tool against them. On the other hand, a nation-state actor might be more concerned with diplomatic losses.

Finally, effective cyber deterrence policies will require regular, sustained disruption of malicious cyber activity. Such disruption should be technical, logistical, legal, financial, diplomatic, and, if necessary, kinetic. Increasing the scope, scale, and cadence of disruption activities would impose real costs on our common adversaries; given the level of malicious activity currently occurring, deterrence will not be credible unless it is backed by clear, decisive action. Further, rather than reaching a steady end-state, cyber deterrence policies should seek to push the digital ecosystem into a dynamic equilibrium. Activity would occasionally increase, necessitating stepped up disruption activity; at other points, activity would drop below the equilibrium level, allowing nations to shift some resources to other problems.

If the United States, its allies, and like-minded nations were to deploy expanded cyber deterrence policies with these five features, doing so could achieve two strategic goals. First, the cyber deter-

rence gap would shrink, effectively expanding the range of deterrable activity. Second, the volume, intensity, and impact of malicious activity that falls within that narrower gap would be reduced.

Counterintuitively, these expanded cyber deterrence policies could narrow the deterrence gap by more clearly defining the acceptable uses and effects of offensive cyber capabilities. Cyber deterrence allows for such a possibility precisely because it does not seek zero use, but instead aims for risk management. By gaining broad agreement on the acceptable uses for offensive cyber capabilities outside of active armed conflict, the inverse would also be true: we would have a better understanding of the actions and effects that are outside the bounds. Such an outcome would enable countries to understand and plan for how offensive cyber operations might be used, and it would provide a benchmark against which to measure nations and other actors. This outcome would also allow like-minded nations to protect not just critical infrastructure services or property from cyber operations, but also to protect other kinds of activity, such as democratic elections. Since not just governments, but a broad, multi-stakeholder coalition would have helped create these definitions, the ability to take legitimate action against those entities pursuing "out of bounds" activities would increase.

These expanded, interlocking cyber deterrence policies would also reduce the level of malicious activity endemic to the digital ecosystem. While the United States and its allies cannot eliminate malicious cyber activity, they can reduce such activities to a manageable level over the long run. Expanded cyber deterrence policies could help achieve this goal by reducing criminal safe harbors, the impact of ransomware, and the use of proxies.

Expanded cyber deterrence policies would shrink the number of countries harboring cybercriminals in two ways. Capacity building already forms a part of cyber deterrence; enhanced policies would dramatically expand these efforts. Therefore, if a country lacks the technical capability to pursue, arrest, and prosecute cybercriminals, then a combination of private sector, NGO, and foreign government resources would provide a backstop. On the other hand, if a country currently perceives harboring criminals as beneficial, then cyber deterrence policies that are more tightly coupled to other, non-cyber interests will alter that calculus. Instead of seeing cybercriminals as a cost-free augmentation of government capabilities, the country would take on some liabilities.

Ransomware has transitioned from an economic nuisance to a national security and public health and safety threat. The level of economic damage, the resources now financing other criminal activities, and the impact to public health and safety have become too large to sustain. Cyber deterrence can play a role in combating this growing threat. As with malicious cyber activity more broadly, cyber deterrence might seem useless against ransomware attacks. However, the multistakeholder Ransomware Task Force sponsored by the Institute for Security and Technology recently released a report with almost fifty policy recommendations for reducing the scope, scale, and impact of ransomware; almost a quarter of these recommendations focused on using deterrence against ransomware.[11] Along with preparedness, disruption, and response, deterrence was one of the four main policy areas in the report. The Task Force embraced deterrence not only as a possibility but as a critical element in the fight against ransomware.

Finally, expanded cyber deterrence policies could help disentangle cybercrime from nation-state activity by discouraging the use of proxies. Since the United Nations Group of Governmental Experts issued its consensus report in June 2013, many governments have come to agree that one norm of responsible behavior in cyberspace is that countries are responsible for malicious cyber activity emanating from their territory, regardless of whether they are aware of such activity before

it occurs.[12] Expanded cyber deterrence policies tied more explicitly to these norms would increase international and multistakeholder pressure on nations to reduce the use of proxies. Coupled with better definitions of acceptable behavior, the ability to use "plausibly deniable" proxies would decrease because nations would be responsible for such behavior. By holding nations more accountable for damages, even if unintended or stemming from supposedly non-state actors, a cyber deterrence initiative could constrain the more profligate use of proxies. This constraint would also encourage nations to be more targeted and cautious in their use of cyber tools, and in turn reduce the impact of these operations on the ecosystem.

As the digital ecosystem becomes ever more integral to the functioning of societies around the world, establishing effective cyber deterrence policies becomes a critical, even existential requirement. Although some scholars have argued that we should abandon the concept of deterrence in cyberspace, without effective deterrence policies cyberspace will become a net liability rather than an asset. The good news is that, while it does not work in the same manner as nuclear deterrence, cyber deterrence already works to some degree. The United States and like-minded nations intent on upholding the agreed norms need to expand deterrence's reach, stopping more malicious cyber activity before it occurs, and they need to reduce the impact of any remaining activity to sustainable levels. Sustained, coordinated cyber deterrence policies that properly account for cyberspace's nature and that have the characteristics outlined above would enable the United States and its allies to better enforce the already agreed to norms of behavior in cyberspace. It could also reduce the impact of cybercrime on our economies and public health and safety. Such an effort can work, but it can only do so through sustained, high-level commitment, and a realization that we cannot solve our cybersecurity problems, we can only manage their risks. But managing those risks effectively would generate huge benefits for everyone.

Endnotes

1 For example, see Richard J. Harknett and Michael P. Fischerkeller. "Deterrence is not a credible strategy for cyberspace." Orbis, June 23, 2017. https://www.fpri.org/article/2017/06/deterrence-not-credible-strategy-cyberspace/.

2 Dina Temple-Raston. "How the US Hacked the ISIS." National Public Radio, September 26, 2019. https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

3 The United States Department of Justice. "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." Office of Public Affairs, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

4 Bill Briggs. "Hackers hit Norsk Hydro with ransomware. The company responded with transparency." Microsoft, December 16, 2019. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/.

5 David Sanger and Nicole Perlroth. "Pipeline Attack Yields Urgent Lessons Abour US Cybersecurity." New York Times, May 14, 2021. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

6 United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security. December 27, 2013. https://undocs.org/A/RES/68/243.

7 The White House. "National Cyber Security Strategy of the United States of America." September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

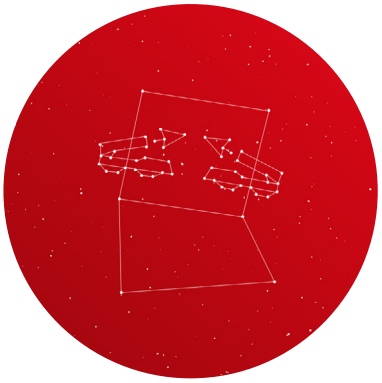
8 The Aspen Institute's Cybersecurity Group published elaborating on this concept: "An Operational Collaboration Framework." Aspen Cybersecurity Group, November 2018. https://www.aspeninstitute.org/publications/an-operational-collaboration-framework/.

9 Add the following reference to endnote ix for that May 2021 GGE report: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf; The Global Commission on the Stability of Cyberspace. Advancing Cyberstability. The Hague: The GCSC, November 2019. https://cyberstability.org/report/.

10 The White House Office of the Press Secretary. "Fact Sheet: President Xi Jinping's State Visit to the United States." Last Modified September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

11 The Institute for Security+Technology. "RTF Report: Combatting Ransomware." Accessed June 17, 2021. https://securityandtechnology.org/ransomwaretaskforce/report/. The Task Force brought together more than 60 people from the private sector, civil society, sharing organizations, and governments for a three month sprint to develop these recommendations.

12 United Nations General Assembly. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." June 24, 2013. https://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf.



About the Author

Michael Daniel serves as the President & CEO of the Cyber Threat Alliance (CTA), a not-for-profit that enables high-quality cyber threat information sharing among cybersecurity organizations. Prior to CTA, Michael served for four years as US Cybersecurity Coordinator, leading US cybersecurity policy development, facilitating US government partnerships with the private sector and other nations, and coordinating significant incident response activities. From 1995 to 2012, Michael worked for the Office of Management and Budget, overseeing funding for the U.S. Intelligence Community. Michael also works with the Aspen Cybersecurity Group, the World Economic Forum's Partnership Against Cybercrime, and other organizations improving cybersecurity in the digital ecosystem. In his spare time, he enjoys running and martial arts.

About the Cyberstability Paper Series

Since the release of the final report of the Global Commission on the Stability of Cyberspace in November 2019, the concept of cyberstability has continued to evolve. A number of new 'conditions' are emerging: new agreements on norms, capacity building and other stability measures have been proposed and solidified within the United Nations and elsewhere, and stakeholders are exploring ways to increase stability and minimize the risk of conflict in cyberspace through technical fixes or governance structures. The constellations of initiatives involved in working towards cyberstability is expanding, underlining the need to connect the traditional state-led dialogues with those of the Internet communities from civil society and industry. Gaps continue to close, between the global north and south, between technology and policy, but also the stability in and the stability of cyberspace.

The first Cyberstability Paper Series explores these "New Conditions and Constellations in Cyber" by collecting twelve papers from leading experts, each providing a glance into past or future challenges and contributions to cyberstability. The papers are released on a rolling basis from July until December 2021, culminating in an edited volume. All papers will be available for open access, and a limited number of printed hardback copies are available.

Published by

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre
for Strategic Studies