Arms Control and International Security Papers
Volume I | Number 20
October 20, 2020

International Security in Cyberspace: New Models for Reducing Risk

by Christopher A. Ford

The Arms Control and International Security Papers are produced by the Office of the Under Secretary of State for Arms Control and International Security in order to make U.S. State Department policy analysis available in an electronically-accessible format compatible with “social distancing” during the COVID-19 crisis.

Arms Control and International Security Papers Volume I, Number 20 | October 20, 2020
International Security in Cyberspace: New Models for Reducing Risk

International Security in Cyberspace: New Models for Reducing Risk

by Christopher A. Ford[1]

In this ACIS Paper, Assistant Secretary Ford recounts the evolution of U.S. cyberspace security diplomacy over the last several years, describing the difficulty of making traditional "arms control" concepts work in this novel domain, but emphasizing the valuable contributions nonetheless already being made through the articulation of voluntary, nonbinding norms of responsible state behavior and a shift to a more explicitly deterrence-focused cyberspace security policy.

In this ever more Internet-connected age, it is no surprise that cyber threats continue to increase. The more indispensable such connectivity is for commerce, communications, and innumerable aspects of daily life, the more that malicious actors see opportunities to steal (or hold hostage) the information lifeblood of our contemporary economy, or otherwise to profit malevolently from modern dependencies. But the problem goes beyond the "ordinary" criminality of fraud and theft, and even the "traditional" cyber espionage undertaken by states.

The emergence of a new era of great power competition has raised the stakes in the cyber arena. Adding to the problems we already faced from cyber criminality, we now also must address a new layer of geopolitical threat from revisionist states such as the People's Republic of China (PRC) and the Russian Federation. These states use cyber tools to steal technology to build up the military capabilities they array against us, to prepare for devastating attacks upon our critical infrastructure in the event of crisis or conflict, to carry out disruptive cyber attacks aimed at destabilizing our allies and partners, and to influence and manipulate our electoral processes. This shift is a challenge of enormous magnitude, and one to which the non-authoritarian world is still only in the early stages of mounting effective responses.

Success in meeting these challenges requires a whole-of-government response, and such a broad response is indeed underway pursuant to the broad guidance provided by the U.S. National Cyber Strategy announced in September 2018. This paper sets forth the work we have been doing to contribute to that strategy at the U.S. Department of State.

I. The Growth of Cyber Threats

We face growing cyber threats from great power competitors, the PRC and Russia, in at least three novel respects: (a) cyber-facilitated technology-transfer; (b) potential disruptive or destructive cyber attacks against critical infrastructure; and (c) cyber-facilitated political manipulation. The first of these, cyber-facilitated intellectual property theft, has been an indispensable component of the PRC's ongoing program to steal foreign technology and put it to use in augmenting the geopolitical and military power

[1] *Dr. Ford serves as U.S. Assistant Secretary of State for International Security and Nonproliferation, and is additionally performing the duties of the Under Secretary for Arms Control and International Security. He previously served as Special Assistant to the President and Senior Director for Weapons of Mass Destruction and Counterproliferation on the U.S. National Security Council staff.*

available to the Chinese Communist Party (CCP). And the scale of such theft is stunning – with former National Security Agency director General Keith Alexander having famously said that "the value of theft of intellectual property from American industry" through the cyber domain "represents the single greatest transfer of wealth in history."

Beyond such ongoing theft and the diversion of stolen U.S. technology and intellectual property, however, we also face growing threats to our critical infrastructure from PRC and Russian efforts to prepare for possible all-out warfare in the cyber domain. There is little that can be said publicly, of course, about the specific nature of the threats they are working to create in this regard – or about the United States' efforts to respond to what we are learning of the problem – except that these challenges are very real.

As the Office of the Director of National Intelligence warned last year in its worldwide threat assessment, the cyber threat to U.S. critical infrastructure has become significant. Already, for instance,

> "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure – such as disruption of a natural gas pipeline for days to weeks – in the United States. …
>
> "Moscow is now staging cyber attack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis …. Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure – such as disrupting an electrical distribution network for at least a few hours – similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage …."

Nor are such warnings merely speculative. Disruptive cyber attacks occurred in both 2015 and 2016 against the electricity distribution system in Ukraine, the global Internet suffered disruption in 2017 as a result of irresponsible and uncontrolled North Korean ("WannaCry") and Russian ("NotPetya") computer viruses, Russia disrupted websites and television stations in the country of Georgia in 2019, and state-sponsored PRC cyber actors have targeted global "cloud" and managed service providers for a number of years.

The trend is clear, and things are worsening. Although most of the disruptive and damaging cyber attacks seen to date have not risen to the level of a use of force, it is possible that a future cyber attack could constitute a use of force or armed attack. So grave is the potential threat that is emerging, in fact, that in the name of deterring the worst such attacks, the U.S. Nuclear Posture Review of 2018 took pains to emphasize that we do not rule out even the possible use of *nuclear weapons* in response to a sufficiently "significant non-nuclear strategic attack" – a term that includes, but is not limited to, "attacks on the U.S., allied, or partner civilian population or infrastructure, and attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities." This is a critical new element in U.S. nuclear declaratory policy, and lest there be any confusion about whether a cyber attack could potentially constitute a "significant non-nuclear strategic attack," I can say with confidence that *it most certainly could* if it caused kinetic effects comparable to a significant attack through traditional means.

Surely not coincidentally, moreover, Russian government officials participating in cyber-related Groups of Governmental Experts (GGEs) at the United Nations have recently tried to walk back aspects of their prior commitment to and acceptance of important declarations (as described below) about the applicability of international humanitarian law (IHL) to cyber operations in armed conflict. Where once Moscow agreed with the common sense and morally inescapable position that IHL principles such as military necessity, proportionality, distinction, and humanity would apply to cyber attacks in wartime just as they apply to kinetic or any other form of attack, now the Kremlin's representatives have begun to equivocate, suggesting that it might be "impossible" to apply IHL in cyberspace because it is hard to distinguish between "civilian" and "military" objects in that domain.

Such claims are false – for it is *not* impossible to apply IHL in cyberspace, and it is not impossibly hard to distinguish between legitimate and illegitimate targets in cyberspace during armed conflict – and are quite alarming, inasmuch as such Russian logic would seem also to justify indiscriminate massacres of civilians during armed conflict if it is "too hard" to distinguish between civilians and combatants. With ongoing Russian efforts to lay the groundwork for attacks using cyber assets against critical infrastructure that supports basic necessities of civilian life, Moscow's effort to retreat from acknowledging the applicability in cyberspace conflict of the IHL principles of necessity, proportionality, distinction, and humanity suggests that the Kremlin is comfortable with *needlessness*, *disproportion*, *indiscriminateness*, and *inhumanity* in contemplating future cyber attacks against civilians.

But even that sort of barbarism is not the end of the story, for the cyber threat we face has evolved also to include efforts to influence and manipulate the very processes of democratic electoral choice that distinguish our system of governance from ugly tyrannies such as Russia and the PRC. According to the 2019 worldwide threat assessment,

> "all our adversaries and strategic competitors will increasingly build and integrate cyber … influence capabilities into their efforts to influence U.S. policies and advance their own national security interests. In the last decade, our adversaries and strategic competitors have developed and experimented with a growing capability to shape and alter the information and systems on which we rely. … They are now becoming more adept at using social media to alter how we think, behave, and decide."

The U.S. Intelligence Community's assessment in 2017 that Russia ran an influence campaign directed at the U.S. 2016 presidential election is well known, and need not be rehashed here except to point out its brazenness – and the fact that such efforts were personally approved by Vladimir Putin:

> "Russian efforts to influence the 2016 U.S. presidential election represent the most recent expression of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations. We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election. … Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations – such as cyber activity – with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"

Nor has Russia abandoned such efforts to interfere. According to the 2019 threat assessment,

> "[o]ur adversaries and strategic competitors probably already are looking to the 2020 U.S. elections as an opportunity to advance their interests. More broadly, U.S. adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine U.S. alliances and partnerships, and shape policy outcomes in the United States and elsewhere. We expect our adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences, suggesting the threat landscape could look very different in 2020 and future elections.
>
> "Russia's social media efforts will continue to focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians. Moscow may employ additional influence toolkits – such as spreading disinformation, conducting hack-and-leak operations, or manipulating data – in a more targeted fashion to influence U.S. policy, actions, and elections.
>
> "Beijing … is expanding its ability to shape information and discourse relating to China abroad …. China will continue to use legal, political, and economic levers – such as the lure of Chinese markets – to shape the information environment. It is also capable of using cyber attacks against systems in the United States to censor or suppress viewpoints it deems politically sensitive. …
>
> "Adversaries and strategic competitors also may seek to use cyber means to directly manipulate or disrupt election systems – such as by tampering with voter registration or disrupting the vote tallying process – either to alter data or to call into question our voting process. Russia in 2016 and unidentified actors as recently as 2018 have already conducted cyber activity that has targeted U.S. election infrastructure …."

As summarized recently by the U.S. official responsible for election-related counterintelligence, moreover,

> "[a]head of the 2020 U.S. elections, foreign states will continue to use covert and overt influence measures in their attempts to sway

> U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process. They may also seek to compromise our election infrastructure for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results. … We are primarily concerned about the ongoing and potential activity by China, Russia, and Iran."

In sum, the various cyber-related threats we face are without precedent in their scope and their severity, and are particularly acute in the context of the environment of great power competition. So what have we been doing about it?

II. Our Responses

Fortunately, this administration has been working hard to meet these threats, including by leading the world in cyberspace security diplomacy. These steps involve a combination of diplomatic outreach to promote voluntary, non-binding norms of responsible State behavior in cyberspace, hard-headed efforts to set in place an increasingly effective framework of deterrence, and organizational changes to posture ourselves for success in meeting these challenges. Before I address those steps, however, it is necessary to note what we are – fortunately – *not* doing.

A. Honesty About the Limits of "Arms Control"

What we are *not* doing is reflexively chasing solutions that cannot address the problems we face in cyberspace. Effective risk reduction in cyberspace is challenged by several important characteristics of the cyber domain: (1) malicious cyber activity can be carried out across a spectrum that spans activities both above and below the legal threshold of a use of force; (2) impending cyber attacks offer few external observables, giving little strategic or tactical warning and complicating the ability to attribute responsibility for an incident and verify compliance with accepted norms of behavior; and (3) the technologies involved in cyber operations, and their ubiquity and often dual-use nature, as well as their possession by both state and non-state actors, make cyberspace tools difficult to define or control, while raising the possibility that efforts to achieve such control would have severe repercussions for innovation and economic development.

This makes effective "arms control," at least as traditionally conceived, difficult or impossible in cyberspace. Traditional arms control thinking, after all,

> "tends to be "prohibitory and regulatory. It aspires to work on the basis of bright-line distinctions and categories – binary oppositions such as 'legal versus illegal' or 'compliance versus noncompliance' – and it can generally be thought of as a system of 'hard' rules. It also tends to be very focused upon *states* and, in arms control applications, upon regulating the availability of *things*: specifically, certain technological tools capable of creating powerfully disruptive effects."

Unfortunately, however, this approach doesn't work very well in protean, rapidly evolving, high-technology domains such as cyberspace. As I have also pointed out with respect to the high-technology domain of outer space, if one aims to limit or ban "weapons" in cyberspace in the way that traditional arms control tries to address other dangerous tools, it is all but impossible to come up with a good definition.

> "Try as one might, there seems to be no way to avoid being damagingly *over*-inclusive (*i.e.*, leading to the prohibition of technologies essential to peaceful civilian and scientific uses …), dangerously *under*-inclusive (*i.e.*, failing to cover entire categories of [potential] weaponry), or both. … Moreover, even if one could *define* the problem, no intelligible scheme for verifying such a prohibition has ever been devised …."

Like outer space, cyberspace:

> "is a domain in which technologies are evolving so quickly, private and governmental actors are intertwined, and definitions of what can be a 'weapon' are so vague, that it is hard to see how traditional, rule-based and legally binding 'prohibitory' approaches to arms control could work."

Accordingly, the United States has long rejected efforts to impose traditional arms control measures on offensive cyber capabilities. Such a stance is especially important given the degree to which Russian and PRC campaigns to promote "arms control" in cyberspace have focused less on actual measures to reduce the risk of conflict involving technical cyber operations than on efforts to *co-opt* arms control rhetoric in support of efforts by those authoritarian regimes to legitimize oppressive controls over the political *content* of Internet communications.

As so often in diplomacy, therefore, *not* doing dumb things is half the battle. With this in mind, we are duly resisting the temptation to engage in quixotic "arms control" efforts in cyberspace, especially when such proposals originate from dictatorial regimes that are themselves engaged in some of the world's most egregious cyber behavior. The U.S. cyberspace security agenda is hardly entirely negative, however, as the following pages will show.

B. Standards of Responsibility and Restraint

One important plank of the U.S. agenda is to promote clear understandings of what constitutes responsible State behavior in cyberspace. As I have explained elsewhere, U.S. diplomats – for more than a decade, in fact, and across three U.S. presidential administrations – have been working with counterparts around the world to articulate and promote such voluntary, non-binding norms.

One of these key principles is the idea that IHL, international human rights law, and indeed the United Nations Charter itself, apply to State behavior in cyberspace in the event of armed conflict. Led by the United States, a broad coalition of diplomats carried the day on this at the 2013 cyber GGE, which articulated by consensus that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful[,] and accessible ICT environment." This conclusion was reiterated by a subsequent GGE in 2015 and both reports have been endorsed by U.N. Member States.

As noted, Russia has recently started to try to walk back its commitment to this principle, but the rest of the world must stand firm and hold Moscow to account for any backsliding. Especially given the potentially enormous stakes for societies around the world that depend upon the Internet and computerized data and communications systems for myriad aspects of daily life – a dependency that will only increase with the advent of the "Internet of Things" – it is of surpassing importance that cyberspace not be allowed to be seen as a wholly lawless, anarchic, "anything goes" domain in the event of conflict. The achievement of the United States and its GGE partners in making this clear was a signal success for cyberspace security diplomacy.

Beyond articulating the applicability of international law, United Nations cyber GGEs have also spelled out voluntary, non-binding norms of responsible State behavior that apply *short* of armed conflict. The consensus 2015 GGE report, for instance, made "recommendations for consideration by States for voluntary, non-binding norms, rules[,] or principles of responsible behaviour" that include the principle that states should not "conduct or knowingly support [cyber] activity … that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." The U.N. General Assembly has by consensus called on all states to be guided by these norms.

These principles are voluntary, non-binding norms rather than legally binding requirements. Nevertheless, they are a major step forward in creating expectations of responsible behavior in the cyber domain to help guide State behavior and encourage restraint and prudence in cyber operations. Such principles are also critical to the other prong of contemporary U.S. cyberspace security diplomacy – deterrence – because one can only penalize, disincentivize, and hopefully deter *irresponsible* cyberspace behavior once everyone understands what it means to be a *responsible* actor in the first place. Our ongoing cyber deterrence work, in other words, piggybacks in important ways upon the excellent work done in those cyber GGE meetings.

C. Deterrence

To be sure, explicit strategies of deterrence are only relatively recent additions to U.S. cyberspace policy. For a while, the United States seemed almost to hope that the mere example of its good-faith engagement with malicious cyber actors such as Russia and the PRC might be enough to persuade them to rein in their bad behavior. In 2013, for instance, the Obama Administration negotiated an agreement with Russia to establish a communications channel for addressing cyberspace problems that would connect the Nuclear Risk Reduction Center (NRRC) at the U.S. State Department to the Ministry of Defense in Moscow.

Such direct, domain-specific channels can indeed be quite valuable, providing a way for parties to communicate about emergent issues in ways that could help them manage crises and prevent inadvertent escalation. While an important step forward, this NRRC-based link did not represent a fully adequate answer because U.S. policy at the time seemingly ignored the element of deterrence. With its protocols for drawing attention to cyber activities originating in the other's territory that rose to the level of national security concern, in fact, it seemed to rest on the idea that communication *alone* could address growing cyberspace threats, as if the Kremlin's malicious cyber activities were simply miscalculations or mistakes that would be stopped if we simply pointed them out.

Any such expectations, however, quickly fell apart in connection with Russia's influence campaign directed at the 2016 U.S. presidential elections. But the "pure communication" approach collapsed not just because it was clumsy in implementation. It failed because the Russian activity in question *wasn't* a misunderstanding or error that might be corrected after having attention drawn to it, but instead a deliberate *policy choice*. Fundamentally, the Obama Administration's approach seems simply to have rested upon a *category mistake*: the somewhat hubristic assumption that the mere use of a communication channel reserved for incidents that rise to the level of a national security concern would carry an implied threat of consequences sufficient to elicit a change in Russian behavior.

Nonetheless, the existence of the NRRC communications link to Moscow specifically tailored for cyberspace-related engagement is a good thing, and may yet be genuinely useful in a cyber crisis. Better still, however, rather than relying upon mere communications and implied threats, the current U.S. administration has learned the lessons of its predecessors' naïveté and has explicitly incorporated elements of *deterrence* into cyberspace security diplomacy. The lessons of the last few years have made clear that having a framework of responsible state behavior is not enough in itself: there must also be *consequences* for violations of such norms.

Our approach builds upon the 2018 U.S. National Cyber Strategy, which made clear that

> "[a]s the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners…. 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."

In support of the overarching U.S. objective of raising the costs and challenges that face our cyber adversaries, the Department of Defense (DoD) has adopted a new and more forward-leaning approach to "defending forward" against malicious cyber activity. According to the 2018 Department of Defense Cyber Strategy:

> "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict ... by leveraging our focus outward to stop threats before they reach their targets."

The State Department has played a leading role in implementing the National Cyber Strategy – in particular, through building the aforementioned Cyber Deterrence Initiative (CDI). On the one hand, we have continued the work described above to promote acceptance and adherence to the U.S.-developed framework of responsible state behavior in cyberspace. On the other, we have worked within the U.S. government and with international partners to build a shared capacity to swiftly impose consequences when our adversaries transgress this framework. Working with interagency colleagues, we have developed policies, processes, and response options that allow us to act quickly. We have also worked closely with likeminded countries to build a flexible model for organizing cooperative responses to significant cyber incidents.

"Attribution diplomacy" is a critical part this work. As I explained at the Foreign Service Institute (FSI) earlier this year,

> "[i]t used to be a sort of popular conventional wisdom that one of the biggest challenges in cyberspace stemmed from the fact that it was essentially impossible to have confidence in the true source of malicious cyber activity. Cyber deterrence, and indeed any sort of response to cyberattack, it was believed, was

> unavailable because one could never really know who had hit you.
>
> "While attribution is certainly very difficult in cyberspace, however, this received wisdom turns out not to be entirely true. For a sophisticated player – and, make no mistake, the U.S. national security apparatus is extremely sophisticated in these respects – it actually is possible to do more by way of attribution than most observers once thought possible. It is sometimes even possible to share enough information with one's friends and partners that they, too, can have a reasonable degree of confidence in the source of an attack. And this gives us additional possibilities not just for more direct forms of response and deterrence, but indeed for cyber diplomacy.
>
> "Our policy and our actions are clear in this respect, and they contribute both to reinforcing norms of responsible behavior and to deterring irresponsible actions. We will 'name and shame' foreign adversaries who conduct disruptive, destabilizing, or otherwise malicious cyber activity against the United States or our partners. And we do."

And we are getting better and better at mobilizing partners to condemn the condemnable. In September 2019, for instance, 28 states joined in a "Joint Statement on Advancing Responsible State Behavior in Cyberspace," which included a commitment to "work together on a voluntary basis to hold states accountable when they act contrary to this framework." In February 2020, 20 individual states – and the European Union as a whole – also joined in condemning the disruptive cyber attack against the country of Georgia mounted in October 2019 by the Russian GRU military intelligence service.

In April 2020, moreover, the United States and several other likeminded countries issued concerted statements in response to an alert issued by the Czech Republic about its detection of impending cyber attacks targeting its health sector, warning that such actions would result in consequences. This was the first time that likeminded states have come together to warn against a specific *future* cyber attack, and we believe our warning had an effect; despite preparatory work by the would-be perpetrators, no major cyber attack ultimately occurred in that case.

Reinforced by the increasing imposition of not just United States but now also European Union sanctions in egregious cyber cases – coupled with "defend forward" activities – this cyberspace security diplomacy is helping to increase the costs and risks faced by the perpetrators of malicious cyber activity. As I told FSI,

> "[p]iece by piece and precedent by precedent, we are building ever-greater support for norms of responsible behavior in cyberspace, and we are making it increasingly likely that the perpetrators of such malicious activity – and their state-level backers – will be identified. Diplomacy is thus at the center of our efforts to hold malicious actors accountable, and U.S. diplomats lead the way."

D. Organization

Finally, the State Department is working to organize to maximize its effectiveness in dealing with cyberspace security challenges. In the policy community, it is all but universally agreed that the Department badly needs a bureau the full-time job of which is to address cyberspace security and emerging technology (ET) issues. The National Security Commission on Artificial Intelligence, for instance, has said this very clearly, and a similar emphasis upon the importance of setting up a State Department cyber bureau has been heard from the Cyberspace Solarium Commission, as well as from experts at think tanks such as the Center for Strategic and International Studies.

We at State agree – emphatically – and this is why Secretary Pompeo notified Congress in 2019 of our intention to create a new Bureau for Cyberspace Security and Emerging Technologies (CSET). Our move to create CSET is based upon the clear-eyed understanding that in addition to the need to ensure that the Department is fully staffed and prepared for the ongoing challenges of cyberspace security diplomacy, we also need full-time specialist expertise to address the security challenges presented by rapid developments in ET areas such as artificial intelligence and machine learning, quantum information science, nanotechnology, biological sciences, hypersonic systems, outer space, additive manufacturing, and directed energy.

The 2017 National Security Strategy, after all, acknowledges that maintaining a competitive advantage in ET is critical to U.S. national security interests and economic growth. Our strategic competitors certainly think so, and they are working as fast as they can to seize advantage in these areas. Within the State Department, however, efforts to address our national security-related concerns in these areas has hitherto been bureaucratically fragmented. For example, cyberspace security diplomacy is handled by the Office of the Cyber Coordinator (CCI), while the Bureaus of Arms Control, Verification, and Compliance (AVC), International Security and Nonproliferation (ISN), and Political-Military Affairs (PM) each have some national security policy responsibilities related to ET. Hitherto, no one bureau has been responsible for ensuring that the State Department develops and ensures the implementation of coordinated diplomatic responses to the national security-related aspects of cyberspace and of current and future ET. Hence the imperative of CSET.

Reporting to the Under Secretary for Arms Control and International Security, CSET will finally allow the State Department to be organized to handle these various security challenges uniformly. In addition to cyberspace security diplomacy, CSET's responsibilities would include: managing the national security issues posed by emerging technologies and critical information infrastructure; developing and implementing the Department's policy positions on this problem set; addressing issues related to state and non-state actor acquisition and misuse of emerging/converging technologies; engaging with international organizations focused on the security aspects of emerging/converging security technologies; coordinating across the Department to ensure a consistent approach to national security concerns related to dual-use or civil/commercial uses of emerging technologies; managing policy development regarding national security implications of emerging technologies; developing proposals for norms of responsible behavior related to emerging technology security issues; and conducting outreach to ensure coordination among key allies and partners to oppose efforts to promote normative frameworks that would be detrimental to U.S. security interests. The new bureau would also develop training programs to ensure that the Department's overseas staff have the knowledge of cybersecurity and emerging technologies needed to effectively represent U.S. concerns in these critical areas.

This was Secretary Pompeo's vision when we notified Congress of our intent to create the new bureau in the summer of 2019. Thanks to the refusal of merely *two* Members of Congress who have kept "holds" upon our creation of the new bureau, however, CSET still does not exist, *nearly a year and half later*. Our adversaries are surely delighted by this, of course, for *their* activities against the United States have faced no "hold," and indeed are accelerating.

One hopes this roadblock is quickly overcome. The State Department badly needs to posture itself against the cyberspace and ET challenges we face. As we remain stymied in our efforts to reorganize and resource our cyber diplomats, other countries – both partners and adversaries – have moved forward to establish analogous institutions. The Department has already done excellent work along the various lines of effort detailed above, coordinating smoothly across multiple bureaus, but we can do better. With CSET, we soon will.

III. Conclusion

The breadth and severity of the cybersecurity threats we face are great, and increasing. Nevertheless, the U.S. Government is now mounting effective responses – not least, here at the State Department, by promoting voluntary, non-binding norms of responsible behavior in cyberspace and working with interagency partners and likeminded states to penalize and deter irresponsible acts. This is a challenging arena, and will require much hard work and attention in the years ahead. But we are now on the right path, and finally making progress.

DEPARTMENT OF STATE ★ UNITED STATES OF AMERICA ★

ARMS CONTROL AND ★ INTERNATIONAL SECURITY ★ T

Arms Control and International Security Papers

The Arms Control and International Security Papers are produced by the Office of the Under Secretary of State for Arms Control and International Security in order to make U.S. State Department policy analysis available in an