Statement of Brandon Valeriano, PhD

Donald Bren Chair of Armed Politics, Marine Corps University
Reader in Digital Politics, Cardiff University
Adjunct Fellow of Cyber Security, Niskanen Center

# "The International Cyber Conflict Threat Landscape"

Cyber Threats Facing America,
Testimony before the United States Senate Committee on Homeland Security and Government Affairs

May 10, 2017

## Cyber Conflict Dynamics[1]

Cyber conflict represents a long-standing threat to the nation and the international system.[2] First clearly articulated in the 1990s, there is evidence of ongoing cyber conflicts at a proliferating rate since at least 2000 (see Figure 1). The cyber challenge is neither new, nor revolutionary. Instead it is a continuation of international rivalries and grievances now also fought in cyberspace. By understanding active cyber operations in their proper context, which is as methods of coercion, we can seek to understand how the international cyber threat landscape works, what challenges will continue to proliferate, and how to fight back by establishing resiliency in cyberspace.

The cyber security threat arena is undoubtedly a critical vulnerability area for all states, but it also represents an opportunity for the modern nation-state in that cyber capabilities can add to state power and reinforce traditional methods of control. All actors in the international system must confront the challenge of digital connectivity, conflict aided by cyber technologies, and the weaknesses exposed by networked infrastructure.

The problem with the cyber security field is that it often takes a micro view of events, focusing on such famous incidents such as the Russian hack during the 2016 election, the Stuxnet operation against Iran, and the Russian attacks on Estonia in 2007. The cyber security landscape is much more than these high-profile incidents. There is a proliferating universe of cyber security incidents, threat actors, and perspectives that portend escalating danger in the domain. Yet, we also witness few incidents that involve escalation and there is rather limited severity evident in each cyber incident to mark this arena as a critical threat to international stability.

Taking a step back and seeking to understand the landscape as it currently stands can provide critical pathways to meeting the cyber security challenge. Only by understanding the macro picture of cyber security landscape can we articulate policy goals to move forward to meet the challenge. Today, I offer an academic empirical perspective of the macro dynamics of the cyber security field. I will explain the construction of cyber threats as coercive tools, the behavior of major threat actors, and pathways toward ensuring that we have a stable cyber future devoid of escalation and overaction, which are common in technology frameworks. While dangerous, the cyber threat landscape also exhibits genuine stability, aided by complexity and restraint which leads to careful action in cyberspace. This relative stability

---

[1] Much of this testimony draws on two research publications, Valeriano, Brandon and Ryan Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press and Valeriano, Brandon, Benjamin Jensen, and Ryan Maness. Forthcoming. *Cyber Coercion: Compellence in the Digital Domain*. New York: Oxford University Press.

[2] I generally avoid the term Cyber War since it is hyperbolic and not at all indicative of the current cyber conflict situation. For there to be war, there needs to be violence and death. We have yet to see this in cyberspace therefore the preferred term to describe ongoing cyber operations is cyber conflict. I also avoid the term cyber-attack since it is so overused to the point that the term is meaningless and can describe any digital attack. Instead we use the term cyber incident and cyber dispute to describe specific cyber operations. See Valeriano, Brandon and Ryan Maness. 2014. "The Dynamics of Cyber Conflict between Rival Antagonists." *Journal of Peace Research*. 51(3): 347-360

and restraint, however, is often in danger of being upset without maintenance, attention paid to individuals as they interact in cyberspace, and the overestimation of potential cyber effects from offensive actions. Make no mistake, political warfare aided by cyber technologies is a threat to the nation-state, but how we react to it (or in some cases overreact), can harm the evident stability displayed to this point.

**The Universe of International Cyber Threats**

There are three key threat actors in cyberspace: states, non-state actors and state-based proxies, and cyber criminals. Each has distinct motivations, abilities, and limitations. It makes little analytical sense to lump them together into one unified cyber threat actor. Behavior varies by actor; motivations are driven by geopolitics, funding sources, or economic gains, and also level of aggression and willingness to cause chaos.

Here I speak mainly of state actors and state-supported cyber proxies. These actors are the most dangerous, prepared, funded, and capable. While there is a willingness of non-state cyber forces, especially terrorists, to use physical force as directed by cyber methods, there is no evidence any of these actors are capable of violent harm. Their limitations in cyberspace generally constrain them to using cyber tools to cause light chaos or as a method of recruitment and promotion. Criminal actors are less likely to seek to cause physical harm and generally are motivated by peer group status or economic gain. The danger is when these forces become skilled enough to be recruited and supported by state-based actors in exchange for protection from prosecution and formal accusation, a practice that happens quite often autocracies.

*State Based Cyber Conflict: Who fights Whom*

Perhaps the most compelling question in the cyber security arena is who is really fighting whom? The perception by many is that digital frameworks allow small powers to challenge major powers. This conjecture is made without evidence and we see few events where small powers seek to punch above their weight (most of these incidents involve North Korea or Iran). Instead, most digital contests are between relatively equal powers such as Pakistan and India, or South Korea and North Korea. We find that cyber conflict is mainly a regional phenomenon, the exception being incidents involving the United States given our global reach and interests.

The idea that the cyber domain allows non-state actors and individuals to challenge states is false. Of course, there will be breaches and intrusions, but this is mainly because the defender has not properly tested its possible avenues of attack and ensured that the systems they built are relatively secure. This is to be expected, as the internet has not been a key pathway to stability as currently composed. The internet was initially constructed to be open, not secure. New avenues such as cloud computing and blockchains are enhancements on old designs, but still introduce weaknesses into the system leaving all digital systems vulnerable.

The cyber domain, if it is to be considered a separate domain of conflict, generally allows state-based actors to continue with normal influence operations but also operating with plausible deniability. Attribution of state-based actors is not difficult in cyberspace. There are many indicators beyond language and IP addresses that might pinpoint digital aggressors. The real issue is with responsibility, who authorized the operations? Actors such as Russia cover digital aggression through compromised or complacent criminal actors. China either

uses its complex network of Communist Party-approved third parties as well as various groups in the People's Liberation Army (PLA). It can therefore become difficult to figure who really authorized what, which is exactly the advantage of cyber operations that our adversaries have been exploiting. It is not much of a secret who is doing what based on target, intent, and method, but it is difficult to establish responsibility for legal or conventional responses according to international law and norms. This is a problem than can only really be solved through on the ground intelligence assets in aggressor countries, in addition to digital forensics.

Cyber conflict has not ushered in a new way of conducting international affairs, only a new way of communicating threats and undertaking aggressive operations. There are no new digital avenues of conflict, we have yet to witness a cyber conflict where the genesis, fight, and resolution all occurred in cyberspace. Cyber conflict only extends traditional rivalry contests over common issues areas (control of space and place, resources, nationalism) to the digital domain.

Cyber methods are typically used as a method of coercion. Within coercion there is either deterrence, which is a status quo operation to prevent something from happening, or compellence operations which seek a change of behavior in the target. Deterrence in cyberspace is problematic as it depends on credibility, the ability to withstand basic attacks, communicating threats clearly to adversaries, and the willingness to display and use cyber weapons. Compellence is more common since it is thought that cyber operations can be a force of leverage to compel an adversary to change behavior. States then utilize cyber tools to create leverage against the opposition and change strategic calculations. The problem is that evidence of behavior change in cyberspace is rare.

*Types of Cyber Conflicts: Disruption Operations*

Cyber disruption operations are short term harassment operations meant to influence the opposition but at the same time, expend minimal effort and require few resources beyond coordination. Seeking to achieve outsized effects through simple operations, these attacks have short term time horizons and represent targets of opportunity against the opposition. The goal is to harass and provoke a change a behavior in the target through the simple escalation of costs associated with continuing to operate in the cyber domain.

Most these cases are website defacements and distributed denial of service (DDoS) operations, which flood servers with requests for information and result in denial of access. Simple email phishing operations that reveal passwords can also be considered disruptions. With basic protections, government associated targets can be hardened to withstand such attacks, but civilians and individuals remain at risk given their general lack of protection and proclivity for making basic mistakes. The recent Google Docs attack that spread quickly through email systems is a common example of this basic level attack that can wreak havoc on unsecure systems.[3]

The goal of these operations is to cause chaos and escalate costs on civilians and other targets to force the state to act. The Russian attack against Estonia in 2007 was an example of such an attack. Little damage was technically done but the Estonia did disconnect internet

[3] https://www.theverge.com/2017/5/4/15544608/google-docs-spam-phishing-email-hack-secure-account (accessed 5/7/2017)

services for a few days as a precaution. While this was traumatic for digitally advanced state, it also caused no long-term damage and did not result in capitulation to Russian demands.

*Types of Cyber Conflicts: Espionage Activities*

Espionage operations are long term activities meant to manipulate information. The goal is either to take, steal or alter information the target has in order to alter the bargaining situation between two parties. One sure way to alter the positional and status dynamics between two states is alter the information one side has on the other, with more access and information leading to greater ability to escalate costs on the opposition by leveraging vulnerabilities.

Espionage activities can also lead to one state adopting stolen technologies to reduce the perceived power gap, largely the goal of Chinese cyber activities. Chinese espionage is motivated by the desire to catch up to the United States in technological and military capabilities, and the large-scale theft of state secrets and intellectual property is a useful shortcut for this goal.

Russian espionage, on the other hand, is focused on the theft of information from private entities and then publishing this information for the public with complacent whistleblowing sites such as Wikileaks. This is technically data manipulation where information is both stolen selectively and also presented in such a way to highlight perceived flaws in the opposition. Altering information and presenting it in a biased manner is the more insidious danger that arises from cyber espionage because it can destabilize the foundations of a state.

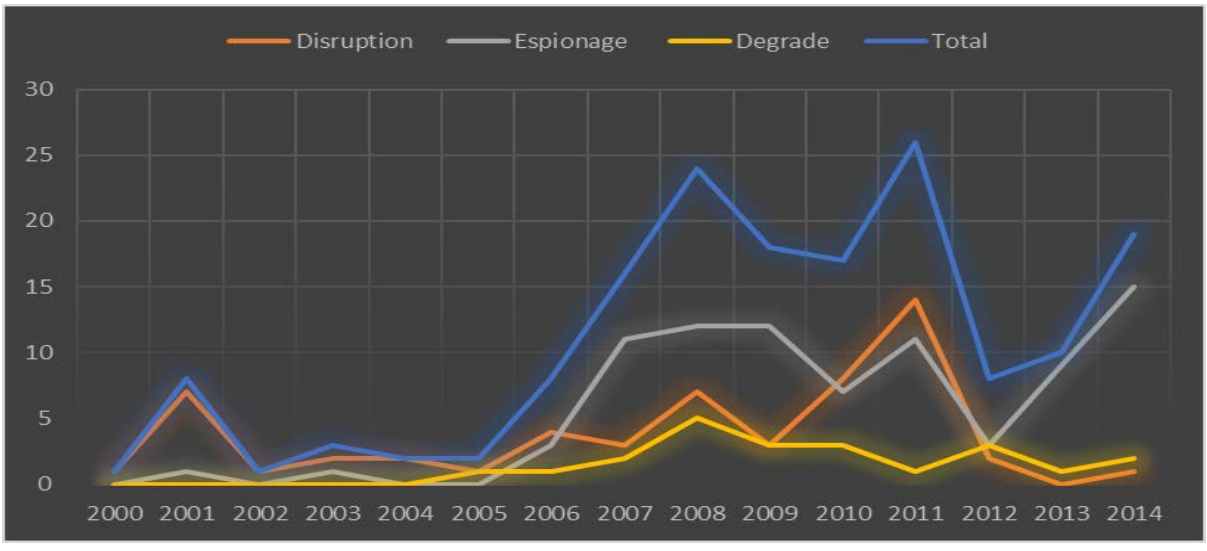


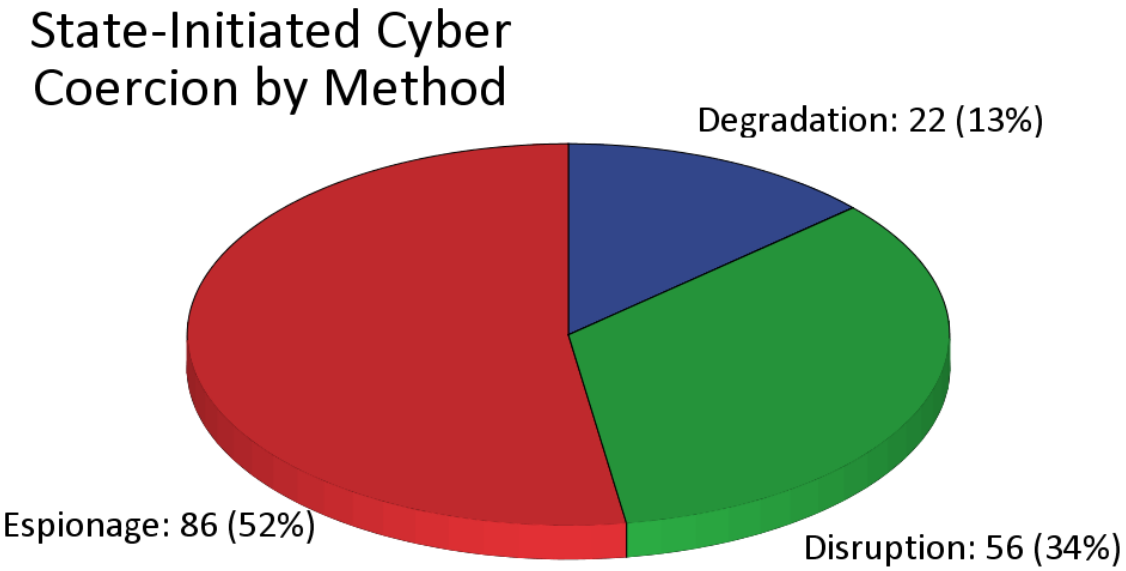

Figure 1: From *Cyber Coercion*, Forthcoming

*Types of Cyber Conflicts: Degrade Campaigns*

Cyber degradation campaigns are potentially the cyber operations with the highest impact, but they are also the costliest, most time intensive, and riskiest. By seeking to degrade the opposition's ability to maintain control of operations, destroy opposition targets, or sabotage procedures, degrade operations seek to punch at the heart of the target to escalate

costs in order to provoke a change in behavior. Such operations have likely been conducted against nuclear facilities (Stuxnet), resource production faculties (Shamoon), and strangely enough, movie studios (Sony Pictures).

These operations are the most famous cyber operations on record but they also attract a disproportionate amount of attention given that they are so rare. As Figure 2 below demonstrates, these coercive cyber events are the rarest of the three categories of cyber coercion. Only 13 percent of known cyber activities overall could be classified as degrade operations, with Figure 1 demonstrating no particular increase in use through time. Our ongoing research also demonstrates that while degrade operations can be effective, they mostly are useful as counterespionage operations. Success rates hover at around 30 percent with is about on par with conventional coercion efforts.




**Cyber Threat Actors**

*Russia*

Russia has demonstrated no great capability in cyber operations. As opposed to media coverage, it often shocking how low tech their techniques are (email spear phishing, tab spamming), and they often fail more than they succeed. However, their evident willingness to conduct political espionage and utilize information warfare tactics is a troubling aspect of Russian behavior for the United States and the West. Russia behavior is paradoxically norm breaking but also simple and near effortless.

In many ways, it seems that Russia is trying to remain relevant and active on the international scene when they have few capabilities to challenge the dominant powers conventionally. Long since caught in a quagmire in Ukraine and unable, so far, to gain traction as they attack European elections, Russia instead seems to be stuck sending cheap

signals towards the digital sky, crying out for attention.

A cheap signal is a method of offering viewpoint that seeks to suggest discontent, but is balanced by the attackers relative inability or lack of interest in pushing the issue further. The methods utilized require little resources, strain, or action. Instead, by using disruption methods, Russia seeks to do the most they can with little effort, akin to flicking at a mosquito with a finger rather than a swatter. The definition of "easy" in cyberspace is to try to affect elections and opinions through email dumps, botnets, and other coordinated influence measures that can be timed and automated.

There can be little doubt that Russia has actively sought to influence elections in the United States, Germany, and most recently France. We cannot normalize this practice, and assume it will continue to happen for any election in the Western world that does not match Russia's grand strategic ambitions. The cyber system we have created enables this process where an aggressor can sit back at home and seek to alter perceptions through simple email dumps and propaganda campaigns.

The only action that can effectively stop the practice is to ignore the curated and biased information released, designate electoral systems critical infrastructure systems, and seek to promote a norm of general revulsion to the practice of releasing private information. This is not to say those attacked do not bear some responsibility, and their systems need to be secure almost to the point of inconvenience. Potential victims also need to accept that digital communications are not private, and active protection needs to be arranged between government cyber operatives and potential political targets much in the same way Secret Service protection is granted to serious candidates.

Challenging Russia on the digital frontier is needed to prevent them from gaining disproportionate influence by utilizing cheap tactics. These tactics can be used right back against them, as the West can employ their own digital armies to counter disinformation with accurate information. But escalating beyond this is needlessly antagonizing, since they seem to the happy enough to continue with a path of least resistance. The Germans have suggested that Russian servers could be wiped out in response to incursions, but this would only invite the same by Russian operatives leading to a spiral of escalation. Even responding with Western troll armies presenting accurate information is potentially norm inducing and blurs the lines of state responsibility.

It must be remembered that Russian influence operations have been attempted in Ukraine in 2014, United States in 2016, and France in 2017 with no discernible effect on actual election outcomes. Each time they failed and generally provoke a reaction that both hardens the target for future attempts but also alerts the next target of the likely incoming attacks. The best way to counter Russia influence is to protect current systems that might provide information and seek to counter their disinformation campaigns with accurate information.

*China*

China employees thousands of hackers and by sheer numbers we would expect a much better yield of their efforts. Instead they seem perfectly content with probing networks and stealing information rather than outwardly expecting to achieve influence through cyber techniques.

China has entered into a cycle of probe, penetration, and retrenchment with the United States. Every few years the United States launches a successful counter-espionage operation that either halts China or forces them to reset their efforts because of the attention placed on them. The United States has also used criminal indictments to decent effect to compel China to change behavior. But this should be countered by the ability of the United States to drive behavior through simple diplomatic exchanges and meetings, such as the agreement on cyber norms between Presidents Obama and Xi in 2015. This led to a cooling off for Chinese espionage operations that has yet to resume.

Countering Chinese cyber espionage is needed but the first obvious step is to shore up Western weaknesses first, third party contractors and weak individuals (insider threats) willing to be bought are the prime vulnerabilities in the United States. As long as the United States has weak links domestically, it will continue to be probed and infiltrated by China.

China does maintain the ability to contest international decisions and actions that they feel go against their interests. They recently have been identified as seeking to infiltrate THAAD missile networks in South Korea.[4] The decision to provide these missile systems to South Korea was obviously contentious and their method of protest and preparation includes cyber infiltrations.

China also maintains active measures to sway public opinion and protest decisions that go against their quest of positive territorial acquisitions in the South China Sea. When operations happen that go against their interests, China can direct its operatives to protest digitally but so far has generally restrained their own activists. These measures are rather tame and to be expected, given the priority these issues have in China.

*Iran*

Iran is thought to be a serious and sophisticated cyber actor but evidence suggests the contrary to this conclusion. The Shamoon attacks on Saudi Arabia's Aramco systems were destructive, but did not impede operations or wipe out critical information. Likely launched in response to the Stuxnet operation, it also telling that the response by Iran was not to attack the alleged perpetrators directly, but to go after an ally indirectly, Saudi Arabia.

Recent attacks on Israel have been reported as another telling aspect of the sophistication of Iranian cyber operations, but the reality is that the state was using released malware from the Shadowbrokers info dumps and spear phishing techniques. Similar attacks on U.S. networks have failed more often than succeeded as well. To argue that these are sophisticated attacks betrays our ability to judge information and impact in cyber security operations.

Ongoing attacks on industrial and financial networks have recently been dubbed Shamoon 2.[5] Reports highlight that the new version of the operation builds on the 2012 attacks on Saudi oil networks and reuses 90 percent of the known code. This is not a highly new or original operation, but a continuation of old methods because targets are slow to

[4] http://thediplomat.com/2017/04/china-based-hackers-targeting-south-korea-over-thaad-report/ (access 5/6/2017)

[5] https://www.scmagazineuk.com/multiple-groups-likely-collaborating-on-shamoon/article/653411/ (accessed 5/5/2017)

update their systems and patch known vulnerabilities.

The main danger from Iran, just as it is in terrorism threat vector, is the high probability that Iran will use proxy actors to attack Western targets. Enabling these actors, one group being called the Syrian Electronic Army, might be dangerous if Iran was to transfer technology to these groups who could then use known vulnerabilities in their operations. But for now, Iran seems content to harass American allies, probe American networks, and reuse old malware to attack unprepared targets.

**Steps Forward to Restore Resilience**

Moving forward to protect the nation requires both the understanding digital threat projections and the recent history of cyber interactions that would match theory with reality. Cyber conflict is not generally new, distinct, or revolutionary. Instead it is a mostly banal continuation of international aggression through digital means. The manipulation of information is the most dangerous aspect of cyber conflict and introduces a new style of political warfare, but we should be not be shocked or unprepared to meet the challenge of cyber conflict.

Education on this recent history is clearly needed, but we often are distracted by the latest attack of the month rather than surveying known past actions. This represents a divorce with typical conflict scenario building where future threats are articulated based on past practices and behaviors. Instead, in the cyber world, we make up new threats, options, and opportunities with little awareness of what has come before or simply just react to the latest news.

*Holistic Cyber Education*

In education and analysis, we focus mainly on cyber actions through technological frameworks and fail generally to enable a general understanding of the cyber threat which would put it in its proper context. That would require building a cyber conflict history background, understand the political motivations for international cyber actions, understanding how rivals engage in conflict, diving into the psychology of cyber behaviors and threat perceptions, knowing the sociology of cyber threat actors, and finally, understanding the biological implications of our networked reality.

As we move forward and think about building a cyber academy on par with West Point or a separate cyber agency, we must remember the general holistic universe of cyber threat actions. This requires us to move beyond just technical understanding of the cyber threat. To do this we must encourage a diverse set of research on cyber issues that is generally not enabled through current National Science Foundation frameworks. Accreditation of cyber education teams by the NSA focuses purely on technical specifications and there is no broader framework to encourage the political, policy, historical, sociological, and biological understanding of cyber security. We will fall behind as a nation until these frameworks are encouraged and maintained.

With the focus on education would also come a much-needed reconceptualization of who operates our cyber security systems. Diversity is a key challenge in these networks as the groups who articulate and monitor critical systems tend to lack diverse perspectives. Diversity is critical in that outcomes are enhanced through diverse thought processes. We

would also need to think about how different types of people access and operate critical systems. The need to expand the cyber work force to include women and ethnic minorities becomes a critical priority. There is no tougher challenge in cyber security than diversifying who is hired to maintain networks and pass on the skills of the past to the future.

*The Human Element*

In attack after attack we witness the key element of weakness is the individual. While the opposition States are undoubtedly malicious actors, their success depends on mistakes and ill-advised behavior of the target. The step in ensuring a secure cyber future would be to focus on protecting the individual and ensure better behavioural process.

Damage in cyber security is often our own making because the greatest impact is psychological rather than reality-based. The overreaction and fear evidenced in reactions to cyber incidents drives the behavior of states seeking to respond to provocations. But can we really respond without shoring up the defensive frontier first? We must first look internally before we blame others for malicious cyber activities.

Basic cyber hygiene is needed, and this extends to the typical recommendations that have yet to be instituted widely: two factor authentication, finger print access, encryption of important machines, and secure card access are all easy adoptable measures that we can do prevent even the most basic attacks. But we also have to take a step back and re-examine processes, such as the high probability that people will click on links because they believe they come from trusted sources, weak web protection in visiting web sites that seek to harvest data, and the high probability that secure systems are accessed from unsecure locations like airports and hotel networks.

As a nation, we have done little at the societal level to reconceptualize how individuals respond to cyber threats. While is there is a much-needed, national conversation taking place regarding the stability of the critical infrastructure network, we have yet to begin a conversation about how re-established personal networks between individuals that can withstand the sure to come cyber-attacks of the future. Resiliency is a national project that requires both awareness of the coming threat but also a fair assessment of the extent and limits of cyber harm.

**Cyber Security for Whom?**

Just who are we seeking to protect? Moving forward and seeking to protect private enterprise is potentially dangerous in that it inserts the state in transactions between private entities. There is little conception of trying to protect the average citizen in cyber security and this remains a core problem with the field.

There are constant probes and intrusions in government systems, they have remained remarkably resilient in the face of cyber challenges. There has been no death and destruction in the domain. Any frame where this would happen generally would occur under the situation of massive war between great powers, hardly the scenarios articulated by cyber security practitioners. What is remarkable about the cyber domain is that despite its existence for over 30 years and during the ongoing wars between a plethora of actors, we have seen few instances of outright digital violence between states. That digital violence between states is

rare might suggest that we have gotten this era of cyber conflict wrong. It is much more stable, constrained and restrained that generally imagined. This would then relocate the danger towards the average citizen rather than the state as a whole.

Moving forward we need a holistic view of the cyber challenge. It cannot be studied as purely a technical domain, but as a domain that critical requires the consideration of the international conflict situation, the motivations of cyber criminals, the psychological impact of the cyber threat frame, the ethics of cyber action, the dynamics of coercion in security frameworks, and finally, the biological impact on human society. Moving beyond the simple war framework would expand just who we seek to protect and what we endeavor to stabilize as we progress with digital communication.

Active measures to defend the nation and go on aggressive attacks are often ineffective and counterproductive outside of counter-espionage operations. There is very little utility in cyber operations to compel the opposition to behave as expected or desired, as these operations might work, but they are costly and enable further digital malevolence by breaking down norms against cyber harm. Cyber deterrence is non-existent and an empty buzzword devoid of real meaning. Proactive measures to ensure a positive cyber future are critical. They include the focus on defensive measures, restoring resiliency in the civilian population, hardening popular targets, and seeking to better understand the process of cyber conflict.

We must strive not to normalize malicious cyber activities. Being hacked is not the price of running a government in the modern international system. It is a perverse outcome of building a structure and system that has little concern for security. Preventing these relatively rare occurrences of cyber violence from becoming common, accepted, and effective is the challenge we face moving forward. The consequences can be drastic in that these tools do not enable liberation technologies, but instead allow moderate reckless powers to seek to compete with stable great powers, allow states to leverage cyber tools to harm activities, protesters, and journalists, and generally seek to further destabilize the international system.

While we have not yet seen the advent of real cyber war and are unlikely to, this does not mean that our future will not be devoid of cyber conflict. In fact, it is becoming quite common and expected as methods of harassment and espionage, basically what Kennan called political warfare so long ago. This active process utilizing cyber tools for attempted coercive effect short of war will only continue to jeopardize our digital futures as cyber technologies fail to become a force for peace and stability but instead symbolize instability and recklessness.