Lessons for Cyber Security in 2017

1) The Importance of the Cyber Threat
2) The Scope of Cyber Conflict
3) Coercion in Cyberspace
4) Norms and the International System
5) Protecting our Future
6) Coming Threats to the Nation
7) The Real Cyber War
8) Steps Forward

The Importance of the Cyber Threat

The cyber threat is invariably a critical threat to the modern nation-state, increasing in scope, and potentially devastating to the ability of a state to conduct the business of commerce, diplomacy, or provide public services. The problem is that this is a threat we must first meet internally by changing our practices and behaviour. The state needs to buff up its defences, promote responsible cyber behaviour, and establish a process of resiliency considering the inevitable cyber-attacks that will continue to come. Responding to cyber aggression with further cyber aggression will not deter attacks, but instead will break the tenuous systems of restrained normative behaviour already established and embroil the nation in conflicts that are not of its choosing.

Cyber security is a high threat to the nation, but it is not the priority or a tier one threat. The main external threats to the state comes from the global economic system post Brexit, terrorism, climate change, and traditional revisionist actors like Russia and North Korea. Cyber security as a threat often is not external in nature, but an internal challenge to establish better practices and behaviours.

Cyber security is also not a domain on its own, but a layer and an additive to other forms of conflict conducted at land, air, in the seas, and in space. Engaging in a battle for cyber domination will only distract from greater issues like reconciliation on other outstanding issues at stake or winning the hearts and minds in a battle for information ascendancy. Isolating cyber as a separate domain will hinder the ability of our organisations to coordinate and integrate digital technologies into their own missions. In some ways, this would be analogous to removing the tank from the army because it is mechanical and instead establishing a mechanical wing of the military. The cyber mission is a complement to traditional forms of state power, rather than an entirely new form of power.

A key tier one threat would be information operations seeking to influence the population. This threat might be associated with cyber means as these methods might provide the information needed to wage an influence battle, but this information can also be

---

I thank Tony Craig for research support. The majority of this evidence was generated from my ongoing and published research, including *Cyber War versus Cyber Realities* (Oxford University Press, 2017) and *Cyber Coercion* (Oxford University Press, Forthcoming), also with Ryan Maness and Ben Jensen. My published work and ongoing research can be found at www.brandonvaleriano.com
manipulated or created. Securing information nodes, establishing trust in government, and maintaining the freedom of the press remain paramount objectives associated with cyber threats.

The reality is that many of the dangers that emanate from the cyber layer involve the problems of the user. Bad basic cyber hygiene, password security, operational security, and extreme overreactions to cyber threats are the genesis of most cyber violations. Research has demonstrated that citizens are just as scared of cyber terrorism as they are of conventional terrorism. This is a strange result since there has not been a significant cyber terror attack, yet these extreme beliefs are likely grounded in our dependence on digital technology. An attack in this arena is a personal violation. We must seek to promote resiliency in the population. We must undertake a national project to reassure citizens of our capabilities and our ability to respond to cyber challenges, to persuade citizens of the public’s need to maintain personal security, and to ensure that legacy systems can fight the coming digital battles.

The Scope of Cyber Conflict

Cyber challenges are not new, revolutionary, or as dramatic as the discourse would lead us to believe. Instead they are typically connected to traditional international challenges such as territorial disputes, rather than new ways of challenging a state. That context matters in cyber security is a fact often missed by the media. Most aggressive actions in cyberspace are a result of real or perceived slights in other domains, such as sabotage or espionage.

While cyber-attacks have increased through time (see Figure 1), we have also seen a remarkable level of restraint by nation-states in their use of the technology. Even China, perhaps one of the most aggressive cyber powers, is leery of using its capabilities for great effect and falls into cycles of espionage attacks and retrenchment when the United States enviably counters. On top this, states that are targeted by cyber-attacks rarely ever respond to such provocations in any domain. Moreover, Russia typically utilises cyber power for harassment, not to degrade the capabilities of the opposition.

Great powers have the power to use cyber for effect, but achieving their ends has been difficult because coercion is difficult in cyberspace and the actors lack the political will to be really disruptive. Degrade operations, those operations seeking to impact the target to a dramatic degree, have generally failed to compel the opposition to change behaviour. Most cyber-attacks that have occurred are disruption (harassment) and espionage attacks. Understanding this process would help us understand how to react to future cyber violations.

![Figure 1: from Valeriano, Maness, and Jensen, forthcoming 2017](image-url)
In terms of a critical infrastructure attack, we need to look at the probability of event occurrence and balance that with imperatives for action. Who would have both the capability and the will to attack the critical infrastructure of a Western nation? Balancing these two factors, it is tough to come up with an aggressor that meets these conditions outside of a direct major power war. We can all dream up a scenario where this might happen but the reality is that this is really a prediction based on little evidence, since major power war has been on the decline for over a generation. A state like Russia would have no interest in engaging in such warfare because it would be out of character as a dramatic escalation outside its sphere of influence, in the post-Soviet Space. A terrorist actor would have the will to undertake such an attack; however, it is dubious that such actors have the ability to conduct a dramatic attack. The capabilities of state actors make them the most dangerous threat, but also make them the least likely aggressors.

Most of my discussion so far has focused on state-on-state cyber conflict. This is prudent since this threat vector is the most dangerous in terms of capabilities, but it does leave out the dangers that emanate from cyber-crime. While cyber-crime can be devastating, this typically has much more to do with the frailties of the companies targeted. The reality is that cyber-crime is not a distinct new way of crime, but a continuation of ancient criminal practices aided by digital technology. The actors, motivations, and goals have remained stable, the only thing that has changed are the methods and technology. This will require a greater effort to train a new generation of law enforcement, but should not lead to a reorientation of national security strategy.

Coercion in Cyberspace: Deterrence and Compellence

Coercion is the process of getting someone to do something they might not otherwise do through either force or the threat of force. Coercion as a term implies either deterrence or compellence. Deterrence is specifically a status quo policy, basically making someone not do something they would otherwise want to do, while compellence is the act of making someone do something they would otherwise not want to do.

Finding a system of cyber deterrence that would work is difficult, the presumption being that digital infiltrations will proliferate unless there is a system setup where the retaliation to an attack would outweigh the benefits. In sort, the costs to the attacker need to be greater than the potential benefits. The idea would then be to increase the costs and demonstrate capability, which would then lead to deterrence.

The problem is that this perception about how deterrence works is at odds with how the current systems of cyber operations are set up. To make known your deterrent strength, it needs to be demonstrated, made credible, and operate in a system where information is communicated. These are three conditions that are often absent in the cyber domain. More critically, for deterrence to work, the target state needs to be able to withstand even the most basic attacks and respond; this ‘defence first’ aspect of deterrence is often missed and needs to become a greater priority.

Credibility is difficult to demonstrate but it implies a state’s willingness to utilise cyber technologies aggressively or to use conventional operations in response to cyber operations. This level of escalation so far has been avoided because the disputes we fight over in cyberspace remain generally minor compared to grander conflicts that drive modern conventional operations. In short, there is no great urgency that drives cyber disputes. The most common violation is cyber espionage and that is an activity every state engages in and will generally have to condone out of mutual guilt: pretty much every state hacks or at least wants to. Cyber disruptions are simple harassment exercises best repaired and ignored.
Degrade operations are rare but are the main incidents that must be prevented because they can compel the opposition to change behaviour if the attack is done to maximum effect and leverages all aspects of state power.

In terms of the offense, establishing a policy of cyber deterrence is an escalatory process. To establish the credibility to deter, you need to demonstrate your weapons in order to scare the adversary with the consequences of action. This would mean that you need to liberally and aggressively use cyber weapons which, in some ways, harkens back to the Madman theory of nuclear weapons where the opposition is scared into non-action because they know the target will be willing to use all options available to respond to a first provocation, even if that means global destruction.

The problem is that Western nations have mainly been restrained in their use of cyber weapons and have not liberally applied cyber force when able, instead holding off where they can because of the high probability that any cyber-attack will affect non-combatants. Utilizing cyber force will essentially mean a degradation in capabilities (once known, the target can defend against the threat), and also would violate norms. No Western nation, besides maybe the United States because of its willingness to conduct cyber espionage and sabotage, is prepared to make a credible case to deter adversaries in cyberspace.

We just need to make clear what expectations we have about behaviour and the consequences of abuses. Deterrence is a buzzword that has no real meaning when applied to cyberspace; reassurance is a better term. No state can deter all cyber actions through the logic of consequences and costs. Instead, we must protect against potential threats and seek to maintain influence operations both at home and abroad to protect against information warfare.

In the realm of cyber crime, deterrence might be more applicable since the state is often willing to persecute abuses when found. The challenge comes with the international nature of cyber crime, where criminals often operate out of locations that do not have formal extradition treaties with the UK. The state should continue to seek to charge individuals committing cyber crime, but whether this will really deter an aggressor located in another country is a different question. The transnational nature of cyber crime is a hindrance, limiting the reach of criminal justice organisations. This then leaves us once again focused on internal protection and seeking better practices that can reassure the public that business can be conducted in the UK safe from criminal interference.

Norms and the International System

The best way to ensure that degrade operations are not conducted against the United Kingdom is to clearly spell out the consequences of such aggression. Deterrence is about escalating costs to prevent action; however, elucidating the consequences of aggression is a different process that seeks to reassure the population that abuses will be dealt with. This is the reality we operate in, since preventing all aggressive actions will be near impossible. The consequences could come in the form of legal sanction and criminal proceedings, termination of trade deals and economic exchanges in the face of cyber espionage, and aggressive institutional responses to sabotage and other events funnelled through a shared sense of collective punishment through a group such as NATO.

It would also be wise to engage in continuing talks to create a normative system of management of cyber aggression through such bodies as the United Nations or NATO, since institutions have traditionally been better able to manage coordinated and credible responses to threats. Yet this effort in the UN Group of Government Experts is fraught with problems of inaction, lack of engagement of key players and a general inability to articulate a common dialogue. Finally, legal standards need to be shared and accepted. The Tallinn Manual has
gone a long way to propose that a system of legal management can occur in cyberspace, but buy in is limited to the West and engagement needs to be expanded.

Escalation, or threat of escalation, is a possible way to push for a system of deterrence that might frighten adversaries into halting aggressive action, but it would also mean an increase in activities in cyberspace. This would throw off the stable system of balance established internationally. Major powers are hesitant to hack for dramatic effect. Most attacks lack the severity of typical events that cause international crises. The Russian hack on the 2016 US presidential election was basically a spear-phishing operation aided by state propaganda. The Black Energy hack on a Ukrainian power plant was stabilised within hours by flipping switches at substations. The 2007 Estonia attack was dramatic, but the impact was made more dramatic by Estonia’s own choice to pull its networks offline rather than battle for control. The continuing US campaign against ISIS in cyberspace is basically an effort to alter and monitor information, not launch cyber bombs as American officials once advocated publicly.

A stable system of restraint has been established internationally. This is not a formal structure of institutions, but the simple acceptance that dramatic infrastructure attacks are off limits to cyber powers. This stability may not hold for long, and surely will not hold during major power war, but we are also not in any immediate danger of this event. The stability we currently have is constructed, maintained, and bolstered by recent legal examinations (Tallinn Manual 2.0) that help create relative stability for a system that is generally unstable.

**Protecting our Future: The Public versus Private Debate**

The public-private nexus in cyberspace is an overused term that has little significance in a global capitalist economy. The state cannot insert itself in the protection of every company as it then becomes responsible for every company. This level of ownership goes beyond conventional standards of assumed responsibility and inserts the state into private transactions. It also is challenged by the multinational composition of most major corporations operating in the UK today.

Privacy issues are commerce issues to be determined by balancing the needs of the corporation with the national security needs of the state. The cyber threat is not yet so devastating that it would generate an imperative to sacrifice our liberties for our security. There needs to be an establishment of clear lines of ownership, protection of critical infrastructure, but also some independence for the IT industry to continue to develop on its own.

Where the state can intervene is in education. It has been done to a limited extent so far, but more needs to be done. There is little monetary reward for establishing a Cyber Centre of Excellence at a university in the UK. If a university were to attain this level of cyber expertise, funding should be pumped into the system so it continues to enhance and grow its capabilities in cyber fields. More outreach and linkages between the intelligence and military organisations in the UK need to be encouraged.

Most of the investment made in the education field comes in the technical aspects of cyber security. While this is critical and important, we also need to bolster the holistic education needed to be a cyber professional. It is near impossible to understand the cyber threat vector without an understanding of international conflict and relations, legal issues associated with technology, and the motivations and genesis of cyber-crime. We need to expand what we think of as cyber education into these critical areas so we can make better policy choices in the future.
Coming Threats to the Nation

The main threat to the United Kingdom comes from information warfare campaigns. While not directly an application of cyber means, information warfare techniques do require a firm foundation of cyber security practices, particularly cyber espionage. Influence campaigns aided with information stolen by cyber means will continue to come. Fighting off this threat requires education, strong internal practices of security, and awareness that external influence is sought on the population.

The hacks during the 2016 presidential election in the United States serve as a warning for us all. The main danger from international actors in cyberspace will come from espionage practices seeking to target liberal democracies. The main challengers are Russia, Iran, and China, each of which seek to delegitimise Western democratic practices.

The Real Cyber War: Cyber Repression

The key challenges in relation to cyber security either involve cyber-crime or cyber warfare. Instead, the more pernicious, complicated, and impactful process is what is likely called cyber repression. Cyber repression is the utilisation of digital tools for harassment, censure, or sabotage of individuals domestically by state actors. The process typically happens in authoritarian regimes, but it is not unknown in advanced democracies. The reality is that we worry about cyber war when journalists, activists, and protestors are surveilled, threatened, and harassed daily via digital means. Amnesty International is constantly hacked, the United Nations is under constant monitoring, and it is difficult to find a working journalist critical of a state like Turkey who is not under digital surveillance and attack.

We know about individual cases but the field of cyber security has not yet turned to meet this challenge, for it is a dramatic challenge to the promise of technology. No longer can we simply believe that technology will aid the human condition and promote democracy, progress, and intellectual thought. Instead, it is likely used more often by nefarious states to further promote state power and maintain a monopoly on violence.

Meeting this challenge will require us to reframe what we think of as cyber security. It will require Western nations to stand up for progress and seek to protect the weakest in society, those seeking to speak out and promote change. We must move beyond the fear of cyber war or even the idea of the internet as a basic human right, but towards the idea that digital harassment is an insidious result of our technological progress. Just as any human rights abuse can be countered, cyber repression can be fought by naming and shaming, sanctions, and raising the issue in diplomatic communications. This would entail documenting such abuses (a process not yet undertaken), providing evidence of such abuses, and challenging those states with repercussions if they continue to harass public individuals. This process could be generally simple if these attacks were conducted while an activist or journalist was working on British soil.

Steps Forward

Moving forward, there are a number of imperative tasks identified in this statement and during the evidence hearing. An immediate task is to conduct stress tests on national critical infrastructure. This would include “red teaming” critical targets, a process whereby a diverse team of experts identifies weaknesses and proposes a way forward. The results may be uncomfortable, but there is an important need to establish a way forward in protecting critical infrastructure. While I may be one of the few that thinks there will not be a coming
“Cyber Pearl Harbor”, I do think it is important to prepare our defences against possible future attacks.

We must also strive to understand and control the human impact of technological vulnerabilities. Why does the citizen react so strongly to cyber actions? Is there a way to promote reassurance and resiliency in the population? Does the average citizen know what the state is doing to protect them from cyber threats? The key challenge moving forward involves people as they are always the weak point in technological processes. More work needs to be done on this area and no country has yet taken an initiative on reassurance operations to promote recovery.

While there is an incredible amount of investment in the cyber security field in the United Kingdom, there is a comparative lack of investment in academia. Our future will be built in the universities, their capacity to train, provide foundations for a global outlook, and think through critical problems to ensure they will remain the critical avenue for the development of a cyber security workforce. We need to strengthen this and invest more in universities that engage in this critical technological challenge. This includes understanding the international relations context of cyber conflict, promoting resiliency in the population, and guiding the government institutions that will rise up to meet the cyber challenge.

Britain will face many cyber security challenges as the technology becomes more ubiquitous. This does not mean that cyber security is a unique challenge to the nation-state, instead it is a challenge like any other – one that can be met with the capacity and indomitable will that the United Kingdom is known for. But there are critical points emerging now. How do we counter information warfare aided by cyber intrusions? What happens once Britain exits the European Union? How does the state meet the challenge to the critical infrastructure and legacy systems? And how do we promote resiliency and recovery in the population? Moving forwards entails meeting new challenges and opportunities, and the UK’s future national strategies for cyber security should therefore be broadened in terms of the scope and the tools that the nation marshals in order to meet the challenge posed by cyber security.

Brandon Valeriano (Ph.D. Vanderbilt University) is a Reader at Cardiff University in the School of Law and Politics. Dr. Valeriano has published dozens of articles in such outlets as the Journal of Politics, International Studies Quarterly, Journal of Peace Research, and International Studies Review. His two most recent books are Cyber War versus Cyber Reality at Oxford University Press (2015) and Russian Coercive Diplomacy at Palgrave (2015). Current research mainly focuses on Cyber Coercion with a book under that title forthcoming in late 2017. He is an adjunct fellow at the Niskanen Center in Washington D.C.