International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain

Brandon Valeriano and Ryan C. Maness

The Oxford Handbook of International Political Theory
Edited by Chris Brown and Robyn Eckersley

Print Publication Date: Mar 2018
Subject: Political Science, Political Theory, International Relations
Online Publication Date: Apr 2018 DOI: 10.1093/oxfordhb/9780198746928.013.19

Abstract and Keywords

Cyber security has undoubtedly become one of the most the significant and proliferating fields of International Relations scholarship. Polls and the news media's reaction to the issue suggest that cyber threats are one of the critical threats in the international agenda, yet scholars have struggled to seriously tackle the implications of this framework and potential theoretical perspectives that would guide inquiry. In this chapter we trace the development of the field, its trends, and the major theoretical ideas suggested by scholars. Our effort will focus on what we know about cyber security and on pressing theoretical questions. The study concludes with an evaluation of the state of norms and ethics in the field given conceptualizations of justice, morality, and norms. Clearly cyber security is an important aspect of international relations; but is the field driving its own ideas, or does it replicate ideas from other security domains?

Keywords: cyberspace, Stuxnet, cyber conflict, cyber defence, cyber capacity

ADVANCEMENTS in technology and the rise of networked machines have perhaps led to the most dramatic changes in social interaction and progress for society over multiple generations. These advances have had important implications for security, given that digital connectivity can be seen both as an opportunity to alter the distribution of power to achieve coercive intent and as a factor contributing to vulnerabilities in states and organizations.

The importance of cyber security as an emerging issue in International Relations (IR) cannot be overstated; what can be overstated is the novelty of the domain. There is a long history of speculation on the role of digital technology in security studies. To some extent originating with Arquilla and Ronfeldt's (1993) concept of netwar and cyber war, there has been an extensive history of theoretical and ethical examinations regarding cyber security concerns. The problem with these past examinations is that they often rely on old frameworks to examine new methods of interaction. Scholarly viewpoints on the cyber se-

curity debate tend to dominated by the popular media's concern with the possibility of global catastrophe brought on by our reliance on technology. The focus has been on the consequences of the technology (Domingo 2015) without first understanding the domain, its coercive potential, and usage by actors.

Technological improvement is continuous and ubiquitous. It impacts our lives because each new advance alters how we communicate and analyse information; it changes how we interact with the world. Change can lead to dependence, and therefore cyber conflict and cyber war have become dominating issues of concern in the realm of international relations. From the telegraph to the telephone, we become dependent on each technological advance, and this dependency creates a perception of vulnerability. (p. 260) Dependence on technology tends to drive the discourse of fear, given the complex nature of technologies. Given the connection between technology, politics, and the military in the domain, technological development remains ripe for theoretical, empirical, and critical examination.

In this chapter, we will evaluate the scope of IR research on cyber security topics with a focus on frames of threat, conflict, power, and ethics. There has been progress in the field, but much remains to be done, given the domain's general lack of theoretical coherence, dependence on frames developed for war frameworks, and general resistance to comparative evaluation.

The Gates Are Down?

The central contention of many scholars in the cyber security field is that the gates are down. In an era of digital connectivity, the state is incapable of maintaining its monopoly on security. This is true: anything networked can be hacked and is vulnerable to infiltration. Yet this is no different any other form of interaction in international politics. Any leader can be killed, any organization seeking to ensure security for the vulnerable can be brought down through internal weakness, dissension, or inaction. Instead of marvelling at the novelty of the cyber domain, the focus of scholarship needs to be on what we know about the domain, how force can be leveraged in the arena, and how to foster the ethical and considered use of power.

Comparative case studies are rare, given the tendency to focus on events that might be outliers, such as the Stuxnet worm (2010), the Sony Hack (2014), and Russia's denial of service bombardment of Estonia (2007). While the atypical events in cyberspace might enlighten our understanding, explaining the everyday and typical in cyber interactions is often overlooked.

The other dominant frame is that of a revolution in military affairs in which technological advances have a dramatic impact on the character and contrast of combat operations. In the cyber context, this is the undertone of Kello's (2013) work that suggests that the future of cyber war will forever change the way states interact with each other. Lindsay (2013) and Gartzke (2013) counter this by noting that there are many constraints on in-

ternational actors to fully employ their advanced cyber weaponry. Technological revolutions are never what they seem, and require appropriate integration with existing technologies to make an impact.

The controversy extends the idea that technology will add to the power and capacity of small states. There are small states such as Estonia and North Korea where this may be the case, but as a collective this claim may be dubious. Estonia wields disproportionate cyber power because of its experience with being attacked in 2007, and is thus now a major centre for cyber defence for the NATO alliance. Lindsay (2013) and Valeriano and Maness (2015: 27) maintain that it is the great powers that will gain the greatest benefit from cyber technologies. Cyber weapons are not simple and cheap weapons to leverage (p. 261) (Valeriano and Maness 2015: 35); they are complicated, expensive, and difficult to utilize for offensive and defense intent.

Many suggested that precision weaponry advanced a revolution and provided an offset and advantage during the Gulf War (1991); but studies since have called into the question the efficacy of precision weaponry, primarily in the context of aerial bombing (Pape 2004; Williams 2010). This suggests that rhetorical arguments on the question must give way to fact-based examinations. There is a great need in the cyber security field to recognize that broad claims without evidence are inadequate, and that the development of theory must be based on more than vague prescriptions for the future.

Definitional Issues

Unfortunately, much time and effort has been spent in the cyber security field exploring the definitions and terms used in the field. “Cyber security” refers to the threat opportunities from digital and computational technologies. Like all frames of security, the idea of perfect protection is a myth; but this is especially relevant for computational-based systems, which will always have weaknesses. The only way to avoid network-based threats is to avoid the drive to network all electronic devices. The more complex question of protection for whom is also often avoided. Most discussions implicitly suggest that the one to be protected is the state, with a focus on critical infrastructure and national industry, but what of the individual or corporation?

Nye’s (2011) definition of cyberspace is useful for political analysis:

> the cyber domain includes the Internet of all networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and political laws of sovereign justification and control.
>
> (Nye 2011: 19)

This layering of cyberspace is critical in the political discourse because it is impossible to leave the state out of the analysis. States still control a monopoly on technology and access through such programmes as the Wassenaar Agreement (limiting access to dual use

technologies). Institutions also play a role, with the International Corporation for Assignment Names and Numbers (ICANN) governing domains on the internet and the United Nations convening several Group of Government Expert's (GGE) reports on cyber security.

The term "cyber power" highlights the continued political importance of computational technologies. Politics is about the distribution of influence, and cyber power is yet another strain of attempts to control leverage, access, and force in international and domestic settings. Valeriano and Maness (2015: 28) define cyber power as the ability to apply typical forms of control and domination in cyberspace. Resources dictate that (p. 262) states continue to have the upper hand in terms of leveraging cyber power (Nye 2010). States still maintain a monopoly on digital violence, and efforts by non-state actors to leverage cyber power often fail.

To date, Stuxnet is the most sophisticated cyber incident ever launched. To slow or deter Iran from developing nuclear weapons, in 2010 a joint US–Israeli effort launched this sophisticated worm in the Iranian Natanz plant, which resulted in the permanent damage of thousands of centrifuges that were enriching uranium. While many take the case of Stuxnet to symbolize the greater vulnerability and power associated with cyber technologies, Lindsay (2013) makes the key point that cyber power is often leveraged by major states to enhance capabilities. This is typical of such states as Russia, China, and the United States, the perceived cyber heavyweights. While other actors like ISIS or Anonymous have been said to leverage cyber capabilities, their ability to demonstrate power has been limited.

The term "cyber war," as used in the discourse, is complicated and loaded. Some, like Lewis (2010), Rid (2013), and Gartzke (2013), argue that cyber war with death associated is unlikely to occur, mainly due to the strategic calculations involved. Valeriano and Maness (2014) observe empirically that cyber war with death as a focus has not occurred and seems unlikely given the general resistance to escalation dynamics (Maness and Valeriano 2016) in cyberspace. If one is going to use the term "cyber war," it should be used correctly, as Rid (2013) points out. "War" as a term implies the use of violence and death to achieve political ends (Clausewitz 2007). War without violence and death is not a war.

We prefer to use the term "cyber conflict" to describe the shape of cyber malice as used in international relations interactions. Cyber conflict is "the use of computational technologies for malevolent and destructive purposes to impact, change, or modify diplomatic or military interactions" (Valeriano and Maness 2015: 21). This definition covers any interactions between entities, including lower levels of malevolence such as disruption and espionage campaigns typical in cyber interactions, all the way to outright cyber warfare—if it were ever to happen.

Nature of the Cyber Threat

Much of the recent trend in cyber security scholarship seeks to evaluate the nature of the cyber threat. As Guitton (2013) notes, accepting the threat inflation framework can have a disastrous effect on policy development. Given that threats seem exaggerated, constructivist frameworks seem to be critical in examining perceptions of cyber threats (Nissenbaum 2005; Hansen and Nissenbaum 2009). The nature of cyber threats and the narratives associated with them are largely socially constructed, and may lead to the securitization of the internet in otherwise free societies.

The work of Dunn Cavelty (2008; 2015) and Lawson (2013) is important in that it reminds us the nature of the cyber threat is often overwhelmed by the extremes in the (p. 263) debate; nuances are more critical than the hyped perspectives typical in the discourse. Concentrated government and private action is needed to contain potential damage, but overestimating the threat will have a similar effect as overestimating the terrorism threat.

Poll data continues to demonstrate that the perception of cyber threat and vulnerability remain at the forefront of public and elite opinion. In an address to Congress in February 2015, US National Intelligence Director James Clapper declared that cyber attacks are a larger national security threat than Sunni extremists, the nuclear ambitions of Iran and North Korea, and Russian and Chinese operatives trying to penetrate the national security community in the United States.

Yet the data collected by Valeriano and Maness (2014) demonstrates a different perspective, observing a low rate of conflict for rival states. Only 20 of the 120 active rival dyads engage in cyber conflict; furthermore, although the number of cyber incidents have been on the rise since 2001, the impact and severity of the incidents have remained constant and at a relatively low level. Nearly three-quarters of these incidents are not coercive in nature, being espionage or disruption in type (Valeriano, Jensen, and Maness 2016).

Axelrod and Iliev (2014) show through game theory and data analysis how one can predict the optimal timing of using cyber resources against adversaries. Certain conditions give states both opportunity and motive to exploit a vulnerability of a target state’s computer system (Axelrod and Iliev 2014: 1298). Using case studies of several high-profile cyber incidents, the study demonstrates that states will wait until the conditions are optimal —but also until stakes are highest—to utilize a cyber resource.

These investigations are important, but they also suggest that context matters. This perspective is that what Langø (2013) calls the environmentalist approach to cyber security, which seeks quantification and analysis in context. The cyber security environment is rich, and deserves scholarship that does not seek to promote an agenda.

The overwhelming majority of cyber conflicts occur between long-standing rivals seeking to harm each other, and exist in the context of regional disputes (Valeriano and Maness 2015). Exploitations between states such as China and Canada are rare, but they do happen. The lesson should be that examinations of the cyber threat and security landscape

are hollow without a deep consideration of and accounting for the international processes. One cannot hope to understand the dynamics of the Sony Hack by North Korea without understanding the long history of rivalry and cultural conflict between the United States and North Korea.

The Nature of Cyber Conflict

The idea that new technologies or ideas can be transformative is both provocative and misleading. Major advances in technology are rarely completely sufficient to bring about doctrinal change, nor are they the tipping point in altering the calculation of military effectiveness. This promise of the future often colours debates and research.

(p. 264) Nowhere is this made clearer than in Kello's (2013) piece, which asserts that current IR theories are unable to contribute in any useful way to the study of cyber conflict, and that the cyber threat remains unprecedented because it will expand the range of harm in international interactions. New theories and new ways of thinking are required, and Kello (2013: 8) asserts that the social science field is ill-equipped to offer anything of value now.

The concept of cyber blockades comes from Russell (2014), who likens certain methods of cyber conflict, primarily distributed denial of service (DDoS), to naval blockades, where the victim state can be economically strangled by its attacker. For example, the 2007 series of defacement and DDoS incidents launched on Estonia from Russia interrupted the daily economic life for many ordinary citizens. This attack was launched because the Estonian government removed a Soviet-era grave-marker; many Russians saw this as an insult, and Russia retaliated with what has been dubbed the first "cyber war." Yet this "cyber blockade" was chosen by the defender to protect systems. The Estonians did not capitulate to Russian demands, and the attack was a brief interlude in relations.

Gartzke's (2013) article about cyber threats and the balance between offence and defense is important in this context. The distinction between what is possible versus what is probable is often missed. Given rational calculations, there is little chance that a state will launch a massive cyber operation even against an enemy due to the limitations of the weapon and the consequences for action.

This is where theory and IR scholarship can have an impact on cyber security research; use of the rational choice and bargaining framework (Gartzke 2013) can temper many of the more bombastic cyber predictions. Likewise, Choucri's (2012) work on international cyber politics utilizes lateral pressure theory to predict how different states with different social, political, and economic traits will behave in the digital realm, suggesting that cyber action is much more complex than the simple ability to launch an attack.

Deterrence and Restraint in Cyberspace

Instead of suggesting that a revolution in military affairs has occurred, Maness and Valeriano (2015) argue that the domain is dominated by restraint rather than by methods of exploitation and escalation. New technologies require new tactics to be developed, but also require support from older methods to achieve victory or exploit weaknesses. A state can steal petabytes of data, yet without the ability to analyse such data this exploit is near-useless (Lindsay 2015: 24). Given the limited nature of training and coordination in major Western states, it is little surprise to find that cyber tactics have been rarely used and are ineffective beyond disruption and information-seeking efforts (Valeriano et al. 2016).

Just what is restraint? Restraint means much more than deterrence. Deterrence has certain limitations that have been shown to be problematic in cyberspace (Libicki 2009). The problems of information, credibility, and variance of the level of cyber actions make (p. 265) it impossible to articulate a system of responses as assured and rigid as deterrence systems built during the Cold War. The connection between cyber security contexts and physical capabilities are said to make deterrence much easier than previously thought (Goodman 2010); yet this frame assumes that conventional deterrence is possible, when many examinations in the past have raised important problems with the theory (George and Smoke 1974; Vasquez 1991).

Restraint is a process of self-containment and straitjacketing that limits the option of response because of consequences of action, not costs as elucidated in deterrence. The flexibility and curve in costs makes defence possible, and the idea that offence is easy when compared to defence depends on the unit under examination.

The US government has “made clear that we respond to cyber attacks in the time, manner and place of our choosing.” This is the language of restraint, not deterrence. Deterrence means assured response such that the attacker figures the costs of an attack are too high. In cyber security, there will likely be a response, but it is no means assured, timely, nor in the domain of the operation in the first place. It is nebulous, flexible, and considered given the implications of civilian harm in cyberspace.

That cyber-capable states like the United States and Russia have refrained from engaging in offensive cyber operations in major conflicts such as in Ukraine, Libya, Syria, Iraq, and Afghanistan is telling (Maness and Valeriano 2015; Geers 2015). Too much focus has been directed to cyber power, as opposed to the more typical option of choosing not to act because of humanitarian issues, legal concerns, the nature of the weapon, and the possibility that it might not be effective in achieving coercive intent.

The Nature of Cyber Power and Force

A great amount of scholarship in cyber security is focused on what might be considered realist theories or their variants, with the concern for power and balance dominating. The question of deterrence is ubiquitous in the domain. The focus generally is on mass destruction and events generally associated with total war—a problematic frame given the general lack of outright violence on the cyber domain (Rid 2011). Although the possibility of death and destruction through cyber events exist, new and novel perspectives are needed to evaluate lower-intensity forms of conflict.

Evaluating the nature of cyber power is a key concern, but this is a tricky proposition, since defensive vulnerability is highly correlated with advanced industrialized societies. States like North Korea and China rank high on defensive capabilities given the closed-off nature of their connections. While the United States is the most powerful cyber state for offensive capabilities, it is also paradoxically the weakest state on the defensive side (Valeriano and Maness 2015: 25). Clarke and Knake (2010: 148) were the first to try to systematically rank cyber power, with North Korea scoring high and the (p. 266) United States scoring low. Russia, China, and Iran are ranked between these extremes in terms of cyber strength. Valeriano and Maness (2015: 25) standardize and extend this effort with modifications that consider how different sectors are protected, how much states engage with others in cyber conflict, and the ratio of connectivity to successful breaches.

This leads us to considerations of the balance of cyber power. Because estimating the nature of cyber power is difficult given the general secrecy in the domain, it is difficult to measure the balance of power, and therefore it is near-impossible to judge whether there is a stable balance of power. The idea that offence dominates in cyberspace is explicit or implicit in many cyber security research articles. Offence is said to be easy and defence difficult, since exploits are easy to buy on the black market, and when they are connected, avenues of attack manifest. In addition, basic cyber hygiene is almost nonexistent in major industrial targets.

This still does not mean that offence dominates, and we prefer to leave this question to empirical evaluation. Some states seem to have mastered defence. Israel is attacked and probed millions of times a day and repels all basic attacks. The United States is likewise probed exhaustively. The violations that do occur tend to come through third-party vendors or contractors.

Lindsay and Gartzke (2015) argue instead that deception may have the advantage in cyberspace. With tactics such as honeypots and traps possible, attackers can be easily tricked. On the other hand, the issue of data integrity is a key future concern, given the possibly that data can be deleted or altered. This idea shifts our conception of power in a new direction, beyond the simple balance between offence and defence, and suggests that these issues are much more complicated in cyber security interactions.

Theorizing about the nature of cyber power is therefore in its infancy. Many assumptions are made about the nature of offence and defence, with little connection to the observed. Nye (2010: 5) notes that because the internet was “designed for ease of use rather than security, the offense currently has the advantage over the defense.” Yet as cyber conflict continues to proliferate, this may not always be the case.

What does seem probable is the rise of proxy actors in cyberspace. As in the arena of terrorism, state actors can use proxy actors to conduct operations and achieve strategic goals (Conrad 2011; Maoz and San-Acka 2012). This is where the attribution and responsibility problem in cyberspace comes to the forefront. Our ability to achieve attribution has been greatly enhanced in recent years (Rid and Buchanan 2014), but deniability can be achieved if proxy actors are used to conduct operations.

The nebulous and disjointed nature of cyber control does pose problems and possibilities. Many major states like Brazil and those in the European Union focus on strength through resilience rather than through offensive capabilities. Violations in cyberspace will always occur; yet the most common vulnerability in all frames of security is often the human actor, and this necessitates a return to the individual level of analysis and considerations of everyday harm in cyberspace. The fear reaction we have built up in this domain dominates (Gross et al. 2015), but it is not clear if this perception should stand out, given the remarkable amount of stability in the system.

(p. 267) Moving beyond frameworks of power, fear, and threat might be opportune at this moment in scholarship. There is a great need to evaluate the nature of cyber espionage (Gartzke 2013; Valeriano and Maness 2015: 4), given that cyber conflict more often than not involves information warfare and disruption, rather than coercion. This then connects cyber security scholarship with the discourses on privacy and surveillance—a needed turn in the field (Rid and Moore 2016).

Cyber Institutions and Governance

What tends to be missed quite often in cyber discourse is the perspective of what might be called liberal theories or institutions. Clear theoretical accounts of the development of institutions that govern cyber interactions are sparse and the field would greatly benefit from regime theory (Choucri et al. 2013).

A multi-stakeholder model, where state-based actors work with corporations and individuals to develop functional models of international governance, does exist, with ICANN being an example (de la Chapelle 2007). Indeed, the interaction between public and private is the key nexus of cyber security relationships in many industrialized economies such as the United States and the United Kingdom. Public–private cooperation to ensure protection of critical infrastructure goes back to the Marsh Commission in 1997. Yet this relationship is complicated, with the state (the public) having difficulty justifying its role, giv-

en concerns about privacy and general misgivings about sharing too much with government.

True multi-level stakeholder methods of governance and representation are needed, especially when many instances of cyber repression, where the state takes actions against individuals, demonstrate the limitations of cooperation between private and public sectors. The promise of the internet as a forum for the development of civil society and democracy promotion has not been achieved, and this might be due to the residual power controls implemented by major powers. Indeed, any model of global governance of the internet must contend with the fact that states are necessary actors in the domain (Cornish 2015).

There is a possibly that the nature of sovereignty (Wendt and Duvall 2008) may change with the introduction of new ideas and concepts. Yet the reality is that the rise of the global internet has not developed into a new global common (Cornish 2015), but instead has prompted extensions of government responsibility and control (Tikk 2011; Demchak and Dombrowski 2011).

Maness and Valeriano (2015) begin to articulate what might start to amount to a liberal preference theory (Moravcsik 1997) in cyber interactions in their examination of the impact of cyber conflict and cooperation at the dyadic level. They find that when a state tries to utilize DDoS attacks or change the behaviour of the enemy, the level of conflict between two states increases. All other attacks, such as intelligence operations or disruption tactics, have a varied and unsystematic impact on relationships. Some states, **(p. 268)** like China and the United States, seem to cooperate more after an attack; this is probably because the issues at stake in cyber actions are of such low salience that they do not provoke antagonistic reactions. This would suggest some fundamental ordering of preferences surrounding cyber actions: only certain actions, such as those that are remarkably public or seek to force someone to change behaviour, are detrimental to relationships.

The Legalist/Moralist Debate

The call for norms of action in cyber security is strong: just about every major statement on cyber security by state leadership tends to invoke a call for shared norms of behaviour. For example, in September of 2015, when Chinese President Xi Jingping was making his state visit to the United States, President Obama remarked, “We’ll work together, and with other nations, to promote international rules of the road for appropriate conduct in cyberspace.”

As the major cyber powers, the United States, China, and Russia, are beginning to formalize agreements on their respective behaviours in cyberspace, empirical analysis (Valeriano and Maness 2015: ch. 4) suggests that informal modes of restrained behaviour have already been employed for at least the last fifteen years. The transition that needs to happen now is to shift these normative outcomes into institutionalized outcomes.

What can be achieved now is the continued encouragement of restrained behaviour by establishing and encouraging a system of justice and proportionality, to mitigate escalation between international actors for the foreseeable future. The Just War tradition may be the optimal existing framework for this new and growing domain, given considerations for harm of innocents (almost assured in the cyber domain, where there is no separation between the military and public) and proportionality (Cook 2010; Valeriano and Maness 2015; see Chapter 16). Adding in moral considerations (Fixdal and Smith 1998) is important, given that the possibility for civilian harm is pivotal in cyber security.

Legal frameworks are often problematic (Goldstone 1998; Spinello 2010; Dipert 2010: 395) and permissive (Eberle 2012). While international legal frameworks can apply to cyberspace (Schmitt 2013), just how different frameworks apply is the subject of much debate. Many reports and investigators seek either to justify offensive behaviour or to explore the novelty of the domain. The Tallinn Manual released in 2013 (Schmitt 2013) was a promising attempt to forge agreement, but differences of opinion remain between state representatives and even between the various authors.

To prevent tragedy (Brown 2007), Valeriano and Maness (2015) propose a system of justice for the use of cyber technologies where states are incentivized to maintain continued restraint. A system of cyber justice can be based on the idea of the Just War tradition, where cyber response is managed and proportional, and where civilian harm is off-limits (O'Driscoll 2008). These practices need continued reinforcement in international forums such as the UN. The goal is to encourage positive cyber practices as a matter of policy.

(p. 269) Conclusion

While the field of cyber security is not new, the intellectual maturity of the perspective is developing. Much of the work to be done in the future requires greater consideration of methods, empirics, and evidence, as well as critical epistemological approaches that would challenge the nature of the institutional arrangements concerning cyber questions. The ethical limitations of cyber actions seem clear, given the potential harm to both civilians and observers. What is needed is greater care in demonstrating the strategic limitations and positive possibilities of cyber actions.

There is much the field can learn from the perspectives of IR theory and ethics. Emerging policy areas need not be filled with reactionary perspectives. Preferring the "island of theory" approach advocated by Guetzkow (1950), no one scholar can attempt to tackle the great majority of cyber security questions. Instead, questions need to be parcelled out and investigated by teams combining skills and abilities. Collaboration and careful relationship-building is needed to achieve progress in this critical domain.

The cyber domain will be an arena continually in need of reset and monitoring, given its importance. International institutions can be a path of stability, as would be controls instituted by hierarchical actors such as the United States, China, Brazil, and the EU. Our evaluation of legal means of control is less hopeful, given the instability of the legal do-

main and the tendency for legal practices to seek to justify potential offensive actions rather than seeking to limit harms.

Given the need to limit harms and violations, ethical perspectives are critical in the cyber domain. The Just War perspective gives us some method of guidance proposing that actions that seek to harm civilians and are not proportional to the violation should be condemned (see Chapter 17). This is the crux of the cyber security debate; there is no separation between civilian space and military targets in cyberspace. Pure military targets are myth: even Stuxnet, an operation directed at a facility in the middle of a desert, was repurposed by non-originating actors.

Due to the importance of the cyber domain to research, education, business, and social interactions, actions in the domain bring great risks but also great possibilities. Anything depended on brings vulnerability, yet vulnerability will not lead to harm in all cases. It can be the path to mutually assured stability, given the importance of digital connectivity. Our cyber futures might not be filled with conflict and violence; as the line between stability and chaos is always in danger of being exploited in cyberspace, the observation that cooperation dominates, despite examples to the contrary, should be reassuring to some extent.

References

Arquilla, J., and D. Ronfeldt (1993). Cyberwar is Coming! *Comparative Strategy* 12(2): 141–65.

Axelrod, R., and R. Iliev (2014). Timing of Cyber Conflict. *Proceedings of the National Academy of Sciences* 111(4): 1298–1303.

(p. 270) Brown, C. (2007). Tragedy, “Tragic Choices” and Contemporary International Political Theory. *International Relations* 21(1): 5–13.

Choucri, N. (2012). *Cyberpolitics in International Relations* (Cambridge, Mass.: MIT Press).

Choucri, N., S. Madnick, and J. Ferwerda (2013). Institutions for Cyber Security: International Responses and Global Imperatives. *Information Technology for Development* 20(1): 96–121.

Clausewitz, C. von (2007). *On War*, trans. J. J. Graham (New York: BN Publishing).

Conrad, J. (2011). Interstate Rivalry and Terrorism: An Unprobed Look. *Journal of Conflict Resolution* 55(4): 529–55.

Cook, J. (2010). “Cyberation” and Just War Doctrine: A Response to Randall Dipert. *Journal of Military Ethics* 9(4): 411–23.

Cornish, P. (2015). Governing Cyberspace through Constructive Ambiguity. *Survival* 57(3): 153–76.

de la Chapelle, B. (2007). Towards Multi-Stakeholder Governance: The Internet Governance Forum as Laboratory. In W. Kleinwachter (ed.), *The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment* (Berlin: Land of Ideas), 256–70.

Demchak, C., and P. Dombrowski (2011). Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly* (Spring): 32–61.

Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics* 9(4): 384–410.

Domingo, F. C. (2015). Review of *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* by Brandon Valeriano and Ryan C. Maness. *Journal of Information Technology and Politics* 2015: 399–401.

Dunn-Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge).

Dunn Cavelty, M. (2015). The Normalization of Cyber-International Relations. In O. Thränert and M. Zapfe (eds), *Strategic Trends 2015: Key Developments in Global Affairs* (Zurich: Centre for Security Studies), ch. 5.

Eberle, C. J. (2012). *Just Cause and Cyber War*. [Online; accessed 19 Apr. 2017.] **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2048447**

Fixdal, M., and D. Smith (1998). Humanitarian Intervention and Just War. *Mershon International Studies Review* 42: 283–312.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War on the Internet Back Down to Earth. *International Security* 38(2): 41–73.

Gartzke, E., and J. R. Lindsay (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies* 24(2): 316–48.

Geers, K. (ed.) (2015). *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO Cooperative Cyber Defence Center of Excellence).

George, A. L., and R. Smoke (1974). *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press).

Goldstone, D. J. (1998). A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech. *U. Colo. L. Rev.* 69 (1).

Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly* 4(3): 102–35.

Gross, M. L., D. Canetti, and I. Waismel-Manor (2015). The Psychological and Physiological Effects of Cyberwar. In F. Allhoff, A. Henschke, and B. J. Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare* (Oxford: Oxford University Press), 157–76.

Guetzkow, H. S. (1950). *Long Range Research in International Relations* (Cambridge: Cambridge University Press).

(p. 271) Hansen, L., and H. Nissenbaum (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53: 1155–75.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security* 38(2): 7–40.

Langø, H.-I. (2013). Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security (Oslo: Norwegian Institute of International Affairs, working paper).

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics* 10(1): 86–103.

Lewis, J. A. (2010). The Cyber War Has Not Begun (Center for Strategic and International Studies). [Online; accessed 19 Apr. 2017.] **http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.pdf**

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar* (Santa Monica, Calif.: RAND).

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22(3): 365–404.

Lindsay, J. R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security* 39(3): 7–47.

Maness, R. C., and B. Valeriano (2015). *Russia's Coercive Diplomacy: Energy, Cyber and Maritime Policy as New Sources of Power* (London: Palgrave Macmillan).

Maness, R. C., and B. Valeriano (2016). Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes? In K. Friis and J. Ringsmose (eds), *Conflict in Cyberspace: Theoretical, Strategic and Legal Perspectives* (New York: Routledge), 45–64.

Maoz, Z., and B. San-Akca (2012). Rivalry and State Support of Non-State Armed Groups (NAGs), 1946–2011. *International Studies Quarterly* 56(4): 720–34.

Moravcsik, A. (1997). Taking Preferences Seriously: A Liberal Theory of international Politics. *International Organization* 51(4): 513–53.

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology* 7: 61–73.

Nye, J. S. (2010). Cyber Power (Belfer Center for Science and International Affairs, Harvard Kennedy School). [Online; accessed 19 Apr. 2017.] **http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf**

Nye, J. S. (2011). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* (Winter): 18–38.

O'Driscoll, C. (2008). *Renegotiation of the Just War Tradition and the Right to War in the Twenty-First Century* (New York: Palgrave Macmillan).

Pape, R. A. (2004). The True Worth of Air Power. *Foreign Affairs* 83(2): 116–30.

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies* 35(1): 1–28.

Rid, T. (2013). *Cyber War Will Not Take Place* (London: Hurst).

Rid, T., and B. Buchanan (2014). Attributing Cyber Attacks. *Journal of Strategic Studies* 38(2): 4–37.

Rid, T., and D. Moore (2016). Cryptopolitik and the Darknet. *Survival* 57(1): 7–38.

Russell, A. L. (2014). *Cyber Blockades* (Washington, DC: Georgetown University Press).

Schmitt, M. (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare (NATO Cooperative Cyber Defence Center for Excellence). [Online; accessed 19 Apr. 2017.] **http://www.ccdcoe.org/249.html**

Spinello, R. (2010). *Cyberethics: Morality and Law in Cyberspace*, 4th edn (Burlington, Mass.: Jones & Bartlett Learning).

Tikk, E. (2011). Ten Rules for Cyber Security. *Survival: Global Politics and Strategy*, 53(3): 119–32.

(p. 272) Valeriano, B., and R. C. Maness (2014). The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11. *Journal of Peace Research* 51(3): 347–60.

Valeriano, B., and R. C. Maness (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press).Valeriano, B., Benjamin J., and R. C. Maness (2016). *Cyber Security: The Evolving Nature of Cyber Power and Coercion* (New York: Oxford University Press).

Vasquez, John A. (1991). The Deterrence Myth: Nuclear Weapons and the Prevention of Nuclear War. In C. W. Kegley (ed.), *The Long Postwar Peace: Contending Explanations and Projections* (New York: HarperCollins), 205–23.

Wendt, A., and R. Duvall (2008). Sovereignty and the UFO. *Political Theory* 36(4): 607–33.

Williams, B. G. (2010). The CIA's Covert Predator Drone War in Pakistan, 2004–2010: The History of an Assassination Campaign. *Studies in Conflict & Terrorism* 33(10): 871–92.

Brandon Valeriano

Brandon Valeriano is the Donald Bren Chair of Armed Politics at the Marine Corps University. He also serves as a senior fellow in cyber security for the Niskanen Center. His three most recent coauthored books are Cyber War versus Cyber Realities, Russia's Coercive Diplomacy, and Cyber Strategy. His ongoing research explores creating comprehensive cyber conflict data, external threats and video games, biological and psychological examinations of the cyber threat, and repression in cyberspace. He received a PhD from Vanderbilt University.

Ryan C. Maness

Ryan C. Maness is an assistant professor of Cyber Conflict and Security in the Defense Analysis Department of the Naval Postgraduate School. His current research explores cyber strategy and coercive effects and how the tactic fits within overall military pg xvistrategies for various countries. His research is based on the collection of cyber events through quantitative methods and is currently constructing a cyber incidents dataset that will not only encompass state actors, but non-state actors as well. He is coauthor of the forthcoming Cyber Strategy: The Changing Character of Cyber Power and Coercion (Oxford University Press), Russia's Coercive Diplomacy: Energy, Cyber and Maritime Policy as New Sources of Power (Palgrave Macmillan, 2015), and Cyber War versus Cyber Realities: Cyber Conflict in the International System (Oxford University Press, 2015). He received his PhD from the University of Illinois at Chicago in 2013.