

Why International Order in Cyberspace Is Not Inevitable

Brian M. Mazanec

Abstract

James Forsyth and Billy Pope argue that great powers will inevitably cooperate and establish rules, norms, and standards for cyberspace. The foundation of their argument is that such an outcome is inevitable because “great powers will have no choice but to cooperate . . . [to] soften the harsh effects of multipolarity and oligopolistic competition.” While it is true that increased competition may create incentives for cooperation on constraining norms, the history of norm evolution for other emerging-technology weapons indicates that such an outcome is unlikely. Forsyth and Pope postulate that the advent of cyberwarfare poses such a range of challenges to states that constraining norms will inevitably take root. On the contrary, norm evolution theory for emerging-technology weapons leads one to conclude that constraining norms for cyberwarfare will face many challenges and may never successfully emerge.

* * * * *

James Forsyth and Billy Pope’s article “Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace” in the Winter 2014 edition of *Strategic Studies Quarterly* addresses a critical question regarding the unfolding age of cyber conflict: will constraining international norms for cyberwarfare emerge and thrive? This is a pivotal question, as highlighted by recent testimony from Director of National Intelligence James R. Clapper, when he stated “the growing use of cyber capabilities . . . is also outpacing the development of a shared understanding of norms of behavior, increasing the chances for miscalculations and misunderstandings that could lead to unintended escalation.”¹ In responding to this question, Forsyth and Pope argue

Dr. Brian M. Mazanec is a senior defense analyst with the US government and an adjunct professor in the School of Policy, Government, and International Affairs in the Department of Public and International Affairs at George Mason University. He has written on cyber and nuclear issues, is the coauthor of the book *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*, and is the author of a forthcoming book on norm evolution theory for emerging-technology weapons.

that great powers will inevitably cooperate and establish rules, norms, and standards for cyberspace.² The foundation of their argument is that such an outcome is inevitable because “great powers will have no choice but to cooperate . . . [to] soften the harsh effects of multipolarity and oligopolistic competition.”³ While it is true increased competition may create incentives for cooperation on constraining norms, the history of norm evolution for other emerging-technology weapons indicates that such an outcome is unlikely.

Forsyth and Pope postulate that the advent of cyberwarfare poses such a range of challenges to states that constraining norms will inevitably take root. On the contrary, norm evolution theory for emerging-technology weapons leads one to conclude that constraining norms for cyberwarfare will face many challenges and may never successfully emerge.

Some of these challenges have been presented by the advent of the other emerging-technology weapons in historic cases such as chemical and biological weapons, strategic bombing, and nuclear weapons. An analysis of these three historic examples offers valuable lessons that lead to the development of norm evolution theory tailored for emerging-technology weapons that can then be applied to cyberwarfare to better evaluate whether or not the authors’ conclusions are well-founded. This article does exactly that, first by defining emerging-technology weapons and norm evolution theory, then briefly reviewing the current state of international norms for cyberwarfare. Next, it illustrates norm evolution theory for emerging-technology weapons—grounded in the three historic case studies—and prospects for current norms among China, Russia, and the United States. Third, it presents a refined theory of norm development as a framework to evaluate norm emergence that contradicts the Forsyth and Pope thesis. This argument leads to the conclusion that a constraining international order in cyberspace is far from inevitable.

Emerging-Technology Weapons and Norm Evolution Theory

Emerging-technology weapons are weapons based on new technology or a novel employment of older technologies to achieve certain effects. Given that technology is constantly advancing, weapons that initially fall into this category will eventually be recategorized as still newer tech-

nologies develop. For example, the gunpowder-based weapons that began to spread in fourteenth-century Europe would clearly have been classified as emerging-technology weapons in that century and perhaps in the fifteenth century, but eventually those weapons were no longer novel and became fairly ubiquitous.⁴ Chemical weapons, up to the early twentieth century, were considered an emerging-technology weapon. Likewise, strategic bombing, up to World War II, also falls into this category. Nuclear and biological weapons were considered emerging-technology weapons during World War II and the immediate years that followed. Today, cyberweapons used to conduct computer network attacks (CNA) are emerging-technology weapons. Forsyth and Pope emphasize “it is useful to recall how other security regimes developed” and even allude to some of these specific historical examples as possible avenues for developing helpful analogies.⁵ Their approach is reasonable, but a systematic review of these historic case studies results in a very different conclusion regarding the prospect for constraining cyber norms.

In general, norm evolution theory identifies three major stages in a norm’s potential life cycle. These three stages are norm emergence, norm cascade, and norm internalization.⁶ The primary hypothesis of norm evolution theory for emerging-technology weapons is that a state’s self-interest will play a significant role and a norm’s convergence with perceived state self-interest will be important to achieving norm emergence and a state acting as a norm leader. It further mentions that norms are more likely to emerge when vital actors are involved, specifically key states acting as norm leaders and norm entrepreneurs within organizations. The United Nations (UN) and the North Atlantic Treaty Organization (NATO) are the two primary intergovernmental bodies and organizations currently being used to promote emerging norms for cyberwarfare. Additionally, there are some other key multilateral efforts to encourage the development of cyber norms, such as the London Conference on Cyberspace and academic cyber norms workshops.

Current Cyber Constraining Norms

Cyberweapons are emerging-technology weapons and have only existed for a short time. There is relative secrecy surrounding most cyber operations with no extensive record of customary practices of states.⁷ Forsyth and Pope make this very point when they highlight that cyber-

space has resulted in a new form of war that “no one can see, measure, or presumably fear.”⁸ While much of the hostile cyber activity to date is not true cyberwarfare but instead is computer network exploitation (CNE) and cybercrime, this should not be interpreted as a customary practice against conducting CNA-style cyberattacks.⁹ Instead, it is evidence of how early we are in the cyber era—akin to the absence of strategic bombing in the first decade of the nineteenth century. Advanced cyberwarfare is only now becoming possible, and a robust target set is emerging as societies become more immersed and dependent on cyberspace. In the absence of firmly established norms governing cyberwarfare, states may also be exhibiting an abundance of caution as they slowly test the limits of what the international community deems acceptable behavior in cyberspace. Of the major CNA-style attacks that have occurred, six are summarized in table 1, including what those attacks may portend for acceptable norms of behavior in cyberspace. The suspected sponsor, target, and effect of the attack are also listed.¹⁰

Table 1: Selected CNA-style cyberattacks: target, effect, and suspected sponsor

<i>Attack Name</i>	<i>Date</i>	<i>Target</i>	<i>Effect</i>	<i>Suspected Sponsor</i>
Estonia	April–May 2007	Commercial and governmental web services (civilian target)	Major denial of service	Russia
Syrian air defense system as part of Operation Orchard	September 2007	Military air defense system (military target)	Degradation of air defense capabilities allowing kinetic strike	Israel
Georgia	July 2008	Commercial and governmental web services (civilian target)	Major denial of service	Russia
Stuxnet	Late 2009–2010, possibly as early as 2007	Iranian centrifuges (military target)	Physical destruction of Iranian centrifuges	United States
Saudi Aramco	August 2012	State-owned commercial enterprise (civilian target)	Large-scale destruction of data and attempted physical disruption of oil production	Iran
Operation Ababil	September 2012–March 2013	Large financial institutions (civilian target)	Major denial of service	Iran

These six CNA-style attacks collectively provide some insight into the emergence of international norms through the customary practice of cyberwarfare. There are three main takeaways from the attacks. First, the majority (four of six) of the attacks were aimed at civilian targets, showing that a norm constraining targeting to explicitly military targets or objectives has not yet arisen. Second, to the extent attacks did strike exclusively military targets, they were suspected to have been launched by Western nations (the United States and Israel). This seems to indicate there may be competing and, in some cases, more permissive norms regarding cyberwarfare depending on which nation is conducting it. This is consistent with the expected competitive environment in the early days of norm emergence. Third, experience with cyberwarfare is very limited at this point. No known deaths or casualties have yet resulted from cyberattacks, and the physical damage caused, while impacting strategically significant items such as Iranian centrifuges, has not been particularly widespread or severe.

While the preceding information makes it apparent that few, if any, normative constraints governing cyberwarfare currently exist, increased attention and discussion—among other things—have helped spurn various efforts to reach consensus on and codify emerging norms for cyberwarfare. However, overall cyber conflict is becoming more destructive, remaining largely covert with limited public discussion, involving an increasing and continued mix of state and nonstate actors, and more US, Russian, Chinese, and Iranian (among others) offensive cyber operations.¹¹ More destructive and sophisticated cyberweapons are likely to be developed, in part due to the success and example provided by Stuxnet and the interest in and proliferation of cyberweapons it has spawned—along with the absence of constraining norms on developing such weapons. As a result, the cost of cyberweapons is likely decreasing as they proliferate and are increasingly employed. Also, cyberwarfare involves a combination of characteristics that make it particularly attractive to states and encourage proliferation of cyberweapons. These special characteristics include the challenges of attribution, the multiuse nature of the associated technologies, target and weapon unpredictability, potential for major collateral damage or unintended consequences, questionable deterrence value, frequent use of covert programs to develop such weapons, attractiveness to weaker powers and nonstate actors as an asymmetric weapon, and use as a force multiplier for conventional mili-

tary operations.¹² They also help explain why the United States, in spite of its interest in developing constraining cyber norms, has continued to pursue secretive military and intelligence CNA capabilities during the past 10 years.¹³ Thus, cyberwarfare capabilities will play an increasingly decisive role in military conflicts and are becoming deeply integrated into states' doctrine and military capabilities. Over 30 countries have taken steps to incorporate cyberwarfare capabilities into their military planning and organizations, and the use of cyberwarfare as a "brute force" weapon is likely to increase.¹⁴ Military planners are actively seeking to incorporate offensive cyber capabilities into existing war plans, which could lead to offensive cyber operations playing an increasingly decisive role in military operations at the tactical, operational, and strategic levels.¹⁵

The Case for Norm Evolution Theory

If the current trends continue, what does norm evolution theory for emerging-technology weapons predict regarding the development of constrictive international norms? Will a consensus of powerful states, as argued by Forsyth and Pope (citing G. John Ikenberry), seek to conserve power through institutional solutions, for example norms, to make their "commanding power position more predictable and restrained"?¹⁶ Or, will norm evolution theory as applied to emerging-technology weapons predict the opposite? The latter is more probable, based on a modified version of norm evolution theory tailored specifically to emerging-technology weapons and historic case studies. The three examples of chemical and biological weapons, strategic bombing, and nuclear weapons are particularly salient historical case studies when considering norm evolution for cyberwarfare due to a variety of reasons.

Chemical and biological weapons and cyberweapons are nonconventional weapons that share many of the same special characteristics mentioned earlier, with significant international security implications. These borderless domain weapons are also attractive to nonstate actors or those seeking anonymity resulting in a lack of clarity regarding attribution. Forsyth and Pope make this point when they mention that nonstate actors "will continue to pose grave challenges to international order within cyberspace."¹⁷

Strategic bombing—particularly with the advent of airpower as an emerging-technology weapon and the early use of airplanes to drop bombs on cities—forced states to grapple with a brand new technology and approach to warfare—as is now the case with cyberwarfare. As with chemical and biological weapons, strategic bombing shares some special characteristics with cyberwarfare. Strategic bombing made civilian populations highly vulnerable, was difficult to defend against, and used technology that also had peaceful applications (air travel and transport)—all of which can also be said about cyberwarfare today. The effort to constrain strategic bombing through normative influences was mixed and at times completely unsuccessful, which makes it particularly well suited as an exemplar of the limits of norms and how other factors may impede or reverse norm development.

Finally, nuclear weapons, like airpower before them and perhaps cyberweapons today, presented states with a challenge of a completely new and emerging war-fighting technology. Nuclear weapons and cyberweapons, like the other emerging-technology case studies, share many of the same special characteristics with significant international security implications, particularly the potential for major collateral damage or unintended consequences (due to fallout, in the case of nuclear weapons) and covert development programs. Because of these common attributes, lessons regarding norm development can be learned and a framework developed that is applicable to predicting the prospects of constraining norms as a tool to address the use of cyberweapons. While at first glance these three historic case studies seem to validate the Forsyth-Pope argument that “great powers will have no choice but to cooperate,” a careful application of the framework based on cyberwarfare predicts a less-promising outcome.¹⁸

Examining how norm evolution theory, informed by the three historical case studies mentioned above, specifically applies to norms for emerging-technology weapons will allow for a more informed prediction regarding the prospects of norm emergence for cyberwarfare. When these three case studies are considered, the primary reason for developing constraining norms for emerging-technology weapons is the perception among powerful or relevant states that such norms are in their national self-interest. That is, a direct or indirect alignment of national self-interest with a constraining norm leads to norm emergence, and the extent to which it is aligned with key or powerful states percep-

tion of self-interest will determine how rapidly and effectively the norm emerges. The role of national self-interest as the primary ingredient leading to norm emergence also helps explain why, when challenged with violations of a young and not-yet-internalized norm, a state is quick to abandon the norm and pursue its material interest by using the previously constrained emerging-technology weapon, as was seen with both chemical and biological weapons and strategic bombing in World War I and strategic bombing in World War II.

Prospects for Cyberwarfare Norms

The key principle of norm evolution theory for emerging-technology weapons is that norm emergence is more likely to occur when powerful, relevant actors are involved, specifically key states acting as norm leaders and norm entrepreneurs within organizations. As mentioned earlier, there are an assortment of intergovernmental bodies and organizations currently being used by a variety of states to promote various emerging norms for cyberwarfare. Through these organizations, varied actors, motivated by a number of factors and employing a range of mechanisms, have promoted various candidate cyber norms, including a total prohibition on cyberweapons and cyberwarfare, a no first-use policy, or the applicability of the existing laws of armed conflict to cyberwarfare. Thus, norm evolution theory would seem to interpret this as a sign of progress for norm emergence. However if one examines these efforts more closely, the prospects are less hopeful.

Powerful States, Constraining Norms, and Self-Interest

Powerful self-interested state actors will play a significant role in norm emergence. Additionally, the perceived state self-interest will be important for norms to emerge and for a state to become a leader of a particular norm. Successful norm emergence requires states as norm leaders. Whether or not, as Forsyth and Pope say, “the structure of international politics will revert to its historical norm, multipolarity,” state calculations of self-interest are unlikely to converge in favor of a constraining cyber norm.¹⁹ After all, there were eight great powers in 1910, and that complicated, rather than fueled, the convergence of a constraining norm for strategic bombing. Since there is generally less exposure or understanding surrounding cyberweapons and actors have different rates of weapon

adoption and cyber vulnerability, states will be reluctant to lead on the issue of norms because they may be unable to determine the utility of such weapons relative to their own interests. However, such calculations are essential if important and powerful states are going to become strong norm leaders and help promote the emerging norm. Additionally, specific to China, Russia, and the United States—the preeminent cyber actors—an analysis of their respective cyber doctrines indicates that there appears to be a perspective that each nation has more to gain from engaging in cyberwarfare than from significantly restricting it or giving it up entirely. Essentially, Forsyth and Pope’s optimism that states will adopt a constraining norm based on intense multipolar competition, increasing dependence on cyberspace, and corresponding investments in information technology (IT) infrastructure is unsupported.²⁰

National investments in cyberwarfare capabilities and the development of doctrine and strategies for cyberwarfare provide insight into state perceptions of self-interest and the expectations for behavior and emerging norms for cyberwarfare. So where do state cyberwarfare programs stand today in China, Russia, and the United States? The three key states discussed here are the most significant, due to the breadth and sophistication of their capabilities and activities and the likelihood that these states are serving as the model for many other nations preparing to operate in cyberspace. These states are the key norm leaders in the emerging multipolar world that norm evolution theory identifies as important to achieving norm emergence. Accordingly, reviewing Chinese, Russian, and US interests and approaches to cyberwarfare is essential to predicting norm evolution and validating or refuting the Forsyth-Pope argument that state interest will converge around constraining international norms.

Chinese Interest in Cyberwarfare

China’s early activity and interest in cyberwarfare indicate that it likely does not consider the emergence of constraining norms in its self-interest. The country has been largely unconstrained by cyber norms and is preparing to use cyberweapons to cause economic harm, damage critical infrastructure, and influence kinetic armed conflict. As such, it is unlikely to be a vocal norm leader. China is best known for its expansive efforts conducting espionage-style cyber operations. For example, in February 2013, the US cybersecurity firm Mandiant released a study

detailing extensive and systematic cyberattacks, originating from Chinese military facilities of at least 141 separate US-affiliated commercial and government targets.²¹ These attacks have led the US Department of Defense (DOD) to classify China as one of “the world’s most active and persistent perpetrators of economic espionage” and to point out that China is also “looking at ways to use cyber for offensive operations.”²² It is this latter point that is of most interest to this article. China is increasingly developing and fielding advanced capabilities in cyberspace, while its interests in cyberwarfare appear to be asymmetric and strategic.

Russian Interest in Cyberwarfare

Like China, Russia’s early cyberwarfare activity—especially the attacks on Estonia and Georgia—indicate that it is largely unconstrained by restrictive cyber norms and is preparing to use cyberweapons in a wide range of conflicts and against a variety of targets. Russia likely does not consider the emergence of constraining norms in its self-interest. As such, one would think the nation unlikely to be a vocal norm leader. However, Russia has been a leading proponent of a total ban on cyberweapons. This is similar to the Soviet Union’s efforts early in the nuclear era to demonize US possession of nuclear weapons while simultaneously pursuing such weapons themselves. This helps illustrate how powerful states acting in their own self-interest can inadvertently act as norm leaders while simultaneously flouting the touted candidate norm. However, Russia’s confusing support for fully constraining norms for cyberwarfare (based on its behavior in the UN and proposal for an “International Code of Conduct for Information Security”) may be based on its broader definition of cyberwarfare and the nation’s interest in using a constraining norm to prevent what it perceives as “propaganda” inside Russia and in its near abroad.²³ However, Russia’s position may also be disingenuous, as it was when supporting the Biological Weapons Convention while simultaneously launching a massive, illicit biological weapons program. To achieve any real convergence among the main cyber actors, the authoritarian interest in constraining free speech must be addressed, which could deflate Russian support.

That the Russian Federation has a general interest in cyberwarfare is widely known. However, outside of the Estonia and Georgia attacks, little is known of Russia’s cyber capabilities. Some believe Russia is a “little too quiet” and that the lack of notoriety is indicative of a high level of

sophistication which enables Russian hackers to evade detection.²⁴ That said, there are some indicators of Russian intent as their doctrine now states that future conflict will entail the “early implementation of measures of information warfare to achieve political objectives without the use of military force, and in the future to generate a favorable reaction of the international community to use military force.”²⁵

US Interest in Cyberwarfare

While China is perhaps the noisiest and Russia the most secretive when it comes to cyberwarfare, the United States is the most sophisticated. The United States is in the process of dramatically expanding its military organization committed to engaging in cyberwarfare and regularly engages in “offensive cyber operations.”²⁶ However, unlike Russian attacks and Chinese planning, the United States appears to exercise restraint and avoids targeting nonmilitary assets. This seems to indicate that the United States is acting as a norm leader for at least a certain category of constraining cyber norms, although the nation’s general “militarization” of cyberspace may be negating the norm-promoting effects of this restraint. While the United States has recently developed classified rules of engagement for cyberwarfare, the nation has articulated few, if any, limits on its use of force in cyberspace or response to hostile cyberattacks. For example, the May 2011 *International Strategy for Cyberspace* states that the United States reserves “the right to use all necessary means” to defend itself and its allies and partners, but that it will “exhaust all options before [the use of] military force.”²⁷ Additionally, former US Deputy Secretary of Defense William Lynn clearly asserted that “the United State reserves the right, under the law of armed conflict, to respond to serious cyberattacks with an appropriate, proportional, and justified military response.”²⁸ Ultimately, the US behavior and interest in cyberwarfare indicate that it does not consider the emergence of robust constraining norms in its self-interest.

Leaks Further Impair States Supporting a Constraining Norm

Edward Snowden’s leaks may have introduced more distrust than had already existed among adversaries and allies alike, complicating and hampering a convergence of norms among states. When reporting began on Snowden’s leaked classified documents, including documents outlining offensive cyberattacks, suddenly the spotlight was on US cyber

activity and the breadth and nature of its thus-far secret offensive actions in cyberspace.²⁹

The purported revelations regarding the extent of the National Security Agency's (NSA) cyberintelligence collection efforts led some US allies, such as Germany and Finland, to begin to construct their own independent IT infrastructure, such as fiber-optic cables.³⁰ Additionally, France has launched its own data countersurveillance efforts. Brazil's president, Dilma Rousseff, cancelled a state visit to the United States, decrying the NSA activities as "an assault on national sovereignty."³¹ This led David DeWalt, chairman of the cybersecurity firm FireEye, to predict that there will be increasing "cyber balkanization" with more cybernationalism and less international cooperation.³² The current Snowden leaks alone will likely have an impact on the evolution of constraining cyberwarfare norms; however, more leaks are likely coming. Future leaks could fracture state interests and increase national secrecy of cyberweapon programs and distrust of US intentions and those of other powerful cyber actors. This type of effect was evidenced by a Russian government source claiming in late 2013 that "Washington has lost the moral authority" in cyberspace and that support for the Russian UN First Committee cyber resolution—titled "developments in the field of information and telecommunications in the context of international security"—was growing and the Group of Government Experts (GGE) becoming more Russian-friendly. It appears that powerful support from self-interested actors has not converged on a comprehensive constraining norm for cyberwarfare, and recent developments may make such a convergence less likely.

Secondary Factors Affecting Norm Emergence

Norm evolution theory for emerging-technology weapons also recognizes secondary reasons for development, such as

- coherence and grafting with existing norms;
- permanent establishment of a norm before the weapon exists or is fully capable or widespread;
- threat inflation regarding the possible effects of the weapon often by the private sector via industry and lobbying groups;

- notions that a weapon cannot be defended against, fueling interest in a norm;
- unitary dominance of a single actor with a particular weapon-type that gives said actor significant influence in norm emergence for that weapon-type; and
- delays in proliferation (often due to technological barriers), creating added time for a constraining norm to emerge.

This comprehensive theory of norm evolution for emerging-technology weapons is a framework for predicting the likelihood of norm development for cyber-related weapons and cyberwarfare and will be used in the remainder of this article to offer additional predictions for cyber norms.

Coherence with Existing Dominant Norms Unlikely

Should current trends continue, the outlook for coherence with existing norms is not favorable when applied to cyberwarfare. First, cyber norms will have difficulty achieving coherence with and grafting onto existing norms. Unfortunately, the success of a norm candidate for emerging-technology weapons also will depend, in large part, on the ability to achieve coherence by connecting the new weapon type to an existing category and thus beginning the process of grafting the new norm onto existing norms. While cyberweapons and cyberwarfare have some commonalities with certain weapons, particularly unconventional and emerging-technology weapons, overall they are truly unique. In fact, they are so unique as to operate in their own new, man-made domain outside the normal domains of land, sea, air, and space. As such, cyber norms lack obvious coherence with many prominent norms; therefore, it is difficult for norm entrepreneurs to graft the candidate norms to existing norms. Perhaps the best option for success is the humanitarian norm underlying the existing laws of armed conflict, particularly the norm regarding the protection of civilians and minimization of collateral damage.³³ This is precisely what NATO's *Tallinn Manual on the International Law Applicable to Cyber Warfare* attempts to achieve, arguing that the laws of armed conflict apply to cyberwarfare.³⁴ However, the lack of agreement on key terms and the confusion over the spectrum of hostile cyber operations make coherence and grafting complex and difficult.³⁵

Too Late to Preemptively Establish Norms for Cyberwarfare

Another challenge for norm emergence is that establishing such norms is generally more successful if the candidate norm can be permanently and preemptively established before the weapon exists or is fully capable or widespread. With cyberwarfare, the train has already left the station so to speak. From 2006 to 2013, James Andrew Lewis of the Center for Strategic and International Studies identifies 16 significant CNA-style cyberattacks.³⁶ These include major attacks across the globe, occurring in such divergent locations as the former Soviet states of Estonia and Georgia and the Middle Eastern states of Iran and Saudi Arabia. While no one has yet been killed by a cyberattack, the opportunity for permanent preemptive establishment of a norm has long since passed.

Differing Perspectives on Future Capability and Threat Inflation

There will be challenges arising from differing perspectives as to future capability and the prospect for threat inflation. While it is true cyberwarfare has been demonstrated to some degree—for example, Stuxnet—the hidden and secretive nature of cyberspace makes the actors and their intent unclear, thus limiting the true demonstrative value of recent cyberattacks. This creates competing theories and arguments as to future effectiveness and strategic impact. Illustrative of this fact, some analysts, policy makers, and academics argue that cyberwarfare poses a major threat and warn of a cyber “Pearl Harbor” or “cyber 9/11” moment when critical infrastructure is attacked. Advocates of the impact and severity of the threat of cyberwarfare have included leading decision makers, such as former US Secretary of Defense Leon Panetta. On the other hand, some have argued that statements such as Panetta’s are pure hyperbole and that cyberwarfare poses no such dire threat and may not even constitute warfare as properly defined. German academic Thomas Rid is the leading advocate of this argument, making the case in his popular book *Cyber War Will Not Take Place*.³⁷ In the December 2013 edition of *Foreign Affairs*, Rid argued that not only is cyberattack not a major threat but also that it will in fact “diminish rather than accentuate political violence” by offering states and other actors a new mechanism to engage in aggression below the threshold of war.³⁸ Others, such as Erik Gartzke, share Rid’s view and argue that cyberwarfare is “unlikely to prove as pivotal in world affairs . . . as many observers seem to believe.”³⁹ However, cybersecurity is a huge and booming busi-

ness for IT-security firms, with industry analyst Deltek reporting that the US federal government IT-security market will increase from \$8.6 billion in 2010 to \$13.3 billion in 2015 (a compound annual growth rate of 9.1 percent).⁴⁰ IT-security expert Bruce Schneier has alleged that these firms benefitting from cyber growth have, along with their government customers, artificially hyped the cyberthreat.⁴¹ Schneier points out these firms have benefitted from the lack of standard terms or understanding of cyberwarfare to conflate a wide range of cyberthreats (CNE, CNA, cyber crime, etc.). Some critics have gone so far as to refer to this dynamic as “cyber doom” rhetoric or a “cyber security-industrial complex” similar to the oft-derided “defense-industrial complex.”⁴² Norm evolution theory applied in this case indicates that these vastly different perceptions as to the impact and role of cyberwarfare in international relations and conflict will impair norm emergence, as was the case early in the twentieth century when the role and impact of strategic airpower was highly contested.

Defenseless Perception Impact

The idea that cyberweapons cannot be defended against will fuel interest in a constraining norm but also limits the effectiveness of reciprocal agreements and can lead to weapon proliferation. As a result, once convention-dependent norms are violated, intense domestic pressure can build for retaliatory violations of the norm. Defenses against cyberweapons are largely viewed as inadequate. A January 2013 report from the DOD’s Defense Science Board indicated that the United States “cannot be confident” critical IT systems can be defended from a well-resourced cyber adversary.⁴³ The nature of cyberspace, with intense secrecy and “zero-day” vulnerabilities makes defense particularly difficult and fuels interest in other strategies to manage the threat, including constraining international norms. This situation explains the broad range of actors and organizations involved in early norm promotion and represents a positive factor for the successful emergence of norms for cyberwarfare. However, the experience of norms for emerging-technology weapons with similar perceptions regarding the weakness of defenses also indicates that, while this may fuel interest in cultivating norms, such norms will be fragile and largely apply to use and not proliferation because actors will continue to develop and pursue the weapons, as those actors believe they cannot rely on defenses and, therefore, seek deterrence-

in-kind capabilities. Further, if the early norm is violated, given the inability to defend against continued violations, there may be domestic pressure to respond in kind, leading to a rapid erosion of the norm. Should early cyber norms be violated, such domestic pressure for an in-kind response could build. In fact, the Iranian attack on Saudi Aramco in August 2012 is largely viewed as one of Iran's responses to Stuxnet.⁴⁴ The challenge of attribution in cyberspace may accentuate this dynamic by making retaliatory responses even easier than with prior emerging-technology weapons.

Unitary Dominance and Delayed Proliferation and Adoption

Finally, weapon proliferation and adoption will play a significant role in norm emergence as it will influence state interest in constraining norms. For cyberwarfare, there is not the kind of unitary dominance of a single actor as there was with the US monopoly early in the nuclear age—giving the United States significant influence on norm emergence regarding nuclear restraint. Additionally, given the ongoing proliferation of cyberweapons, the multiuse nature of the technology, and the relatively low cost of entry, delays in proliferating cyberweapons are unlikely. However, there will likely be varied rates of adoption of cyberweapons, with some nations such as the United States, China, Russia, and Israel possessing the most sophisticated cyber warheads.⁴⁵ Experience with norm development for emerging-technology weapons indicates that states with powerful cyberweapons are more likely to resist the emergence of any constraining norms. This is especially true with strong bureaucratic actors, such as the NSA in the United States or the Federal Agency of Government Communications and Information in Russia, potentially advocating for permissive norms. While the Russians have been major advocates in the UN for a total prohibition on cyberweapons, their interest may be driven by a perception that the United States is the dominant cyberpower, or, perhaps more cynically, it could be akin to the Soviet Union's disingenuous early promotion of the constraining biological weapon and nuclear norms while simultaneously pursuing biological and nuclear weapons. Regardless, the varied rates of adoption and development of cyber capabilities indicates that there will be divergent perspectives on constraining norms, making consensus difficult. This helps explain why despite the many actors and organizations involved in developing candidate norms for cyberwarfare, no success

has been made in achieving any broad consensus beyond perhaps the budding consensus regarding the theoretical application of the laws of armed conflict.


Ultimately, if current trends continue, norm evolution theory for emerging-technology weapons predicts that the emergence and early development of constraining norms will be challenged and may not occur at all. Key states—especially China, Russia, and the United States—are unlikely to perceive the emergence of robust constraining norms as being in their self-interest. Further, limited options for coherence and grafting, inability to preemptively establish a prohibition, lack of unitary dominance, increased proliferation and adoption of cyberweapons, and the lack of powerful self-interested state actors converging on a candidate norm present serious hurdles for norm emergence. However, the connection with the idea that cyberweapons cannot be adequately defended against and industry and government hyping of the threat have spurned significant general interest in constraining norms for cyberwarfare—leading to a rise of many actors and organizational platforms. To move past this point and achieve success, a consensus on cyber norms will need to emerge, and such a consensus does not seem inevitable at this point or in the near future. When it comes to cyber norms, the Forsyth and Pope comment that “hopeful statements most often heard do not coincide with current state practice” will remain applicable for years to come.⁴⁶

Prospects for Cyberwarfare Norm Cascade and Internalization

While norm evolution theory for emerging-technology weapons predicts low odds for constraining cyberwarfare norms, should such norms emerge it is worth briefly examining what the theory predicts about achieving a norm cascade and internalization. These latter two phases in the norm life cycle are important if a norm is to have a structural impact on the international system, as hoped for by Forsyth and Pope. If a constraining cyber norm emerges and approaches a norm cascade, then a tipping point may actually be more likely. Certain indicators are important to achieving a norm cascade, such as potential technological improvements that mitigate the attribution challenge, the unconventional characterization afforded cyberweapons, and the expansive international

arms control and disarmament bureaucracy. However, should the norm cascade occur, internalizing it will be less likely—largely due to secrecy and the multiuse nature of cyber technologies that pose their own barriers to internalization and blunt international pressure for conformity and private-sector support. As a result, norm internalization is likely to be most successful for norms governing usage rather than development, proliferation, and disarmament.

Conclusions

Cyberwarfare is still in its infancy, and there are multiple possibilities for how this new mode of warfare will evolve over the coming decades. However, reasonable conclusions can be drawn regarding the prospects for the emergence of a constraining norm for cyberwarfare. While Pope and Forsyth argue that “so long as the society of states exist . . . the great powers will inevitably leverage cyberspace to enhance rather than undermine its existence” and will have “no choice but to work together” and develop constraining norms, norm evolution theory based on historical case studies involving other emerging-technology weapons predicts otherwise.⁴⁷ The theory indicates there are many hurdles facing development of constraining norms for cyberwarfare and predicts that, if current trends continue, constraining norms for cyberwarfare will have trouble emerging and may not ever reach a norm cascade. This is principally due to the fact that powerful state actors are unlikely to perceive a convergence between a robust constraining norm and their self-interest. While the norm evolution theory for emerging-technology weapons predicts grim prospects for the evolution of constraining cyber norms, the threat of cyberwarfare is unfortunately not diminishing. Realizing that constraining norms are unlikely to develop into a regime that could, as predicted by Forsyth and Pope “strengthen legal liability, reduce transaction costs, and mitigate uncertainty,” is helpful, as it allows policy makers to instead focus on more fruitful strategies for addressing this growing threat.⁴⁸ 

Notes

1. Statement of James R. Clapper, director of national intelligence, “Worldwide Threat Assessment of the US Intelligence Community,” unclassified testimony before the Senate Se-

lect Committee on Intelligence (Washington, DC: 12 March 2013, online), 1, <http://www.intelligence.senate.gov/130312/clapper.pdf>.

2. James Wood Forsyth Jr. and Billy E. Pope, "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace," *Strategic Studies Quarterly* 8, no. 4 (Winter 2014): 113–30, http://www.au.af.mil/au/ssq/digital/pdf/winter_14/forsyth.pdf.

3. *Ibid.*, 114.

4. John Norris, *Early Gunpowder Artillery: c. 1300–1600* (Ramsbury, UK: Crowood Press, 2003).

5. Forsyth and Pope, "Structural Causes and Cyber Effects," 124.

6. Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917.

7. Gary Brown and Keira Poellet, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 126–45.

8. Forsyth and Pope, "Structural Causes and Cyber Effects," 118.

9. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32.

10. While there are more cases of CNA-style attacks than those summarized here, such as the recent attacks on Ukraine and Sony, these were selected as a representative sample of attacks from the key CNA-actors for which there is available open-source information. Any sample selected for this purpose will of course be nongeneralizable and is only useful for identifying general trends and insights.

11. Jason Healey, *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 86.

12. Gregory D. Koblentz and Brian M. Mazanec, "Viral Warfare: The Security Implications of Cyber and Biological Weapons," *Comparative Strategy* 32, no. 5 (November 2013): 418–34.

13. Jason Healey, "How Emperor Alexander Militarized American Cyberspace," *Foreign Policy*, 6 November 2013, <http://foreignpolicy.com/2013/11/06/how-emperor-alexander-militarized-american-cyberspace/>.

14. James Andrew Lewis and Katrina Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (Washington, DC: Center for Strategic and International Studies, 2011); and Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies* 35, no. 3 (June 2012): 401–28.

15. Jason M. Bender, "The Cyberspace Operations Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations," *Small Wars Journal*, 5 November 2013, <http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner>; and Bruce Baer Arnold, "Cold War to Cyber War, Here's How Weapon Exports Are Controlled," *Conversation*, 8 December 2013, <http://theconversation.com/cold-war-to-cyber-war-heres-how-weapon-exports-are-controlled-21173>.

16. Forsyth and Pope, "Structural Causes and Cyber Effects," 115.

17. *Ibid.*, 127.

18. *Ibid.*, 114.

19. *Ibid.*, 119.

20. *Ibid.*, 116–17.

21. William Wan and Ellen Nakashima, "Report Ties Cyberattacks on U.S. Computers to Chinese Military," *Washington Post*, 19 February 2013, <http://articles.washington>

post.com/2013-02-19/world/37166888_1_chinese-cyber-attacks-extensive-cyber-espionage-chinese-military-unit.

22. Anna Mulrine, "China Is a Lead Cyberattacker of US Military Computers, Pentagon Reports," *Christian Science Monitor*, 18 May 2012, <http://www.csmonitor.com/USA/Military/2012/0518/China-is-a-lead-cyberattacker-of-US-military-computers-Pentagon-reports>.

23. Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Secretary-General, letter, A/66/359, 12 September 2011, http://cs.brown.edu/courses/csci1800/sources/2012_UN_Russia_and_China_Code_o_Conduct.pdf.

24. Kenneth Geers, Darien Kindlund, Ned Moran, and Rob Rachwald, *World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks* (Milpitas, CA: FireEye, Inc., 2014), 12, <https://web.archive.org/web/20150123081946/https://www.fireeye.com/content/dam/legacy/resources/pdfs/fireeye-wwc-report.pdf>.

25. Russian Presidential Executive Office, *Военная доктрина Российской Федерации* [Military doctrine of the Russian Federation] (Moscow: Russian Presidential Executive Office, 5 February 2010), https://web.archive.org/web/20150216094415/http://news.kremlin.ru/ref_notes/461.

26. Healey, "How Emperor Alexander Militarized American Cyberspace."

27. Barack Obama, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: White House, May 2011), 14, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; and Ellen Nakashima, "In Cyberwarfare, Rules of Engagement Still Hard to Define," *Washington Post*, 10 March 2013, http://www.washingtonpost.com/world/national-security/in-cyber-warfare-rules-of-engagement-still-hard-to-define/2013/03/10/0442507c-88da-11e2-9d71-f0feafdd1394_story.html.

28. William J. Lynn III, "The Pentagon's Cyberstrategy, One Year Later," *Foreign Affairs*, 28 September 2011, <http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later>.

29. Barton Gellman and Ellen Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-operations in 2011, Documents Show," *Washington Post*, 30 August 2013, http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_print.html; and Kurt Eichenwald, "How Edward Snowden Escalated Cyber War with China," *Newsweek*, 1 November 2013, <http://www.newsweek.com/how-edward-snowden-escalated-cyber-war-1461>.

30. Tero Kuittinen, "NSA Spying Has Triggered a Crazy Chain Reaction of Countermeasures," *BGR*, 16 December 2013, <http://bgr.com/2013/12/16/nsa-spying-finland-fiber/>.

31. Ibid.; and quoted in Kathleen Hennessey and Vincent Bevins, "Brazil's President, Angry about Spying, Cancels State Visit to U.S.," *Los Angeles Times*, 17 September 2013, <http://articles.latimes.com/2013/sep/17/world/la-fg-snowden-fallout-20130918>.

32. David DeWalt, "Going There: The Year Ahead in Cyber Security," *Re/code*, 5 February 2014, <http://recode.net/2014/02/05/going-there-the-year-ahead-in-cyber-security/>.

33. Martha Finnemore, "Cultivating International Cyber Norms," in *America's Cyber Future: Security and Prosperity in the Information Age*, vol. 2, ed. Kristin M. Lord and Travis Sharp (Washington, DC: Center for a New American Security, June 2011), 99, http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf.

34. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

35. Brown and Poellet, "The Customary International Law of Cyberspace," 141.
36. Based on author's analysis of James Andrew Lewis, "Significant Cyber Events since 2006," *Center for Strategic and International Studies* (web site), 11 July 2013, http://csis.org/files/publication/150309_Significant_Cyber_Events_List.pdf.
37. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, April 2012).
38. Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs* 92, no. 6 (December 2013): 77–87, <http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace>.
39. Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013), 42, http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136.
40. John Style and Angie Petty, *Federal Information Security Market, 2010–2015* (Herdon, VA: Deltek, November 2010), <https://iq.govwin.com/corp/library/detail.cfm?ItemID=13648>.
41. Bruce Schneier, "Threat of 'Cyberwar' Has Been Hugely Hyped," *CNN*, 7 July 2010, <http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/>.
42. Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy" (working paper, Mercatus Center, George Mason University, Washington, DC, April 2011), http://mercatus.org/sites/default/files/WP1124_Loving_cyber_bomb.pdf; and "Is Cyberwar Hype Fuelling a Cybersecurity-Industrial Complex?," *Russia Today*, 16 February 2012, <http://rt.com/usa/security-us-cyber-threat-529/>.
43. United States Department of Defense, *Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: DOD, January 2013), 1, <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>.
44. Nicole Perloth, "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, 23 October 2012, <http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html>.
45. As evidenced by the examination of customary state practice of cyberwarfare reviewed earlier in this article.
46. Forsyth and Pope, "Structural Causes and Cyber Effects," 125.
47. *Ibid.*, 123.
48. *Ibid.*, 125.

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.