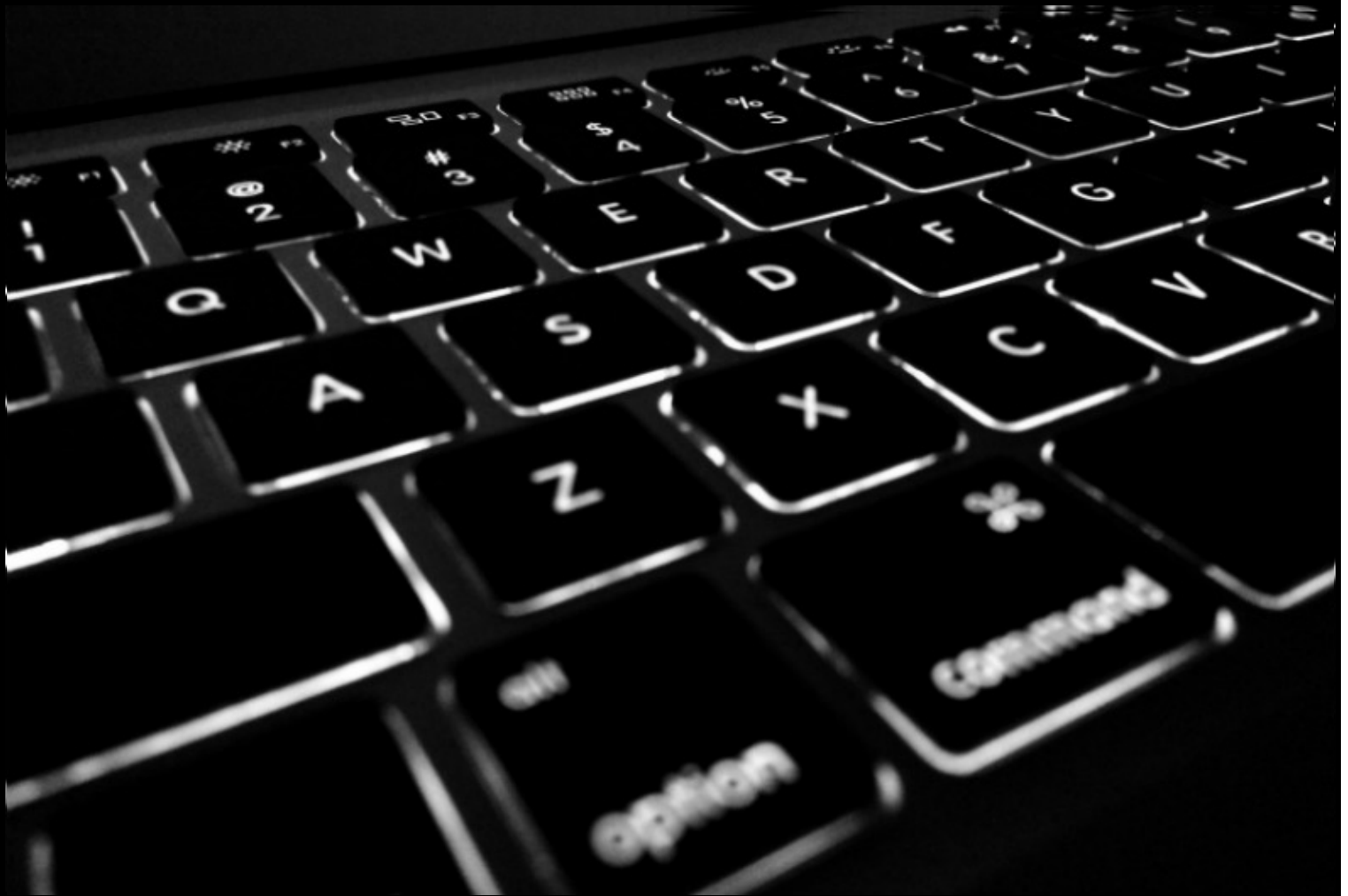




Understanding Cyberwarfare

Lessons from the Russia-Georgia War



Sarah P. White
March 20, 2018



Understanding Cyberwarfare: Lessons from the Russia-Georgia War



Capt. Sarah P. "Sally" White is a cyberspace operations officer in the US Army. She is currently pursuing her PhD in the Harvard Department of Government, where her research interests include military innovation and comparative cyberspace doctrine. She has served in the 82nd Airborne Division and the 780th Military Intelligence Brigade (Cyber). Following graduate school, she will serve as an instructor in the West Point Department of Social Sciences.

Cyberattacks had become an established tool of statecraft by the time they were used against the Republic of Georgia in the summer of 2008, albeit one without a legal framework and whose long-term implications remained poorly understood.¹ Nevertheless, the war between Russia and Georgia that took place in August of that year was remarkable for its inclusion of a series of large-scale, overt cyberspace attacks that were relatively well synchronized with conventional military operations. Conducted by an army of patriotic citizen hackers, the cyber campaign consisted of distributed denial of service (DDoS) attacks and website defacements that were similar in nature but different in method to what had occurred in Estonia the year prior. In total, fifty-four news, government, and financial websites were defaced or denied, with the average denial of service lasting two hours and fifteen minutes and the longest lasting six hours.² Thirty-five percent of Georgia's Internet networks suffered decreased functionality during the

attacks, with the highest levels of online activity coinciding with the Russian invasion of South Ossetia on August 8, 9, and 10.³ Even the National Bank of Georgia had to suspend all electronic services from August 8–19.⁴ While there is strong political and circumstantial evidence that the attacks were encouraged by the Russian state, definitive technical attribution—and thus definitive legal culpability—have remained elusive.

The cyberattacks had little effect on conventional forces and were not decisive to the outcome of the conflict,⁵ but they nevertheless offer significant lessons on the character of modern warfare for scholars of conflict and military studies. This paper will offer a brief analysis of several of those lessons. First, the attacks reinforced the Russian interpretation of cyberspace as a tool for holistic psychological manipulation and information warfare. By impeding the Georgian government's ability to react, respond, and communicate, the cyberattacks

¹ Examples of the state-sponsored use of cyberattacks prior to 2008 include espionage (e.g., Titan Rain, Moonlight Maze), support to precision military raids (e.g., Operation Orchard), sabotage (e.g., Stuxnet, the planning for which is estimated to have begun in 2007), and coercion (e.g., Estonia). Several books provide an accounting of these and other events, to include Segal, *Hacked World Order*; Kaplan, *Dark Territory*; and Healy, *Fierce Domain*.

² Tikk et al., *Cyber Attacks against Georgia*.

³ Russell, "Georgia-Russia War."

⁴ Ibid.

⁵ Interviews conducted with members of the Georgian military, government, and defense ministry, June 2017, in the Republic of Georgia, reinforced the point that while the cyberattacks added a layer of chaos to the Georgian response, they did not affect military decision making about the crisis in a significant way.

created the time and space for Russia to shape the international narrative in the critical early days of the conflict. Second, the attacks highlighted the role of third forces on the modern battlefield. These forces ranged from the citizen hackers who perpetrated the attacks to the private companies who were relied on to defend against them. And third, the attacks provide a useful demonstration of how the technical concepts of cyberspace can be understood through conventional operational concepts in order to more effectively integrate them with military operations.



Cyberattacks in the Russia-Georgia War Reaffirm the Russian View of Cyberspace as a Tool for Psychological Manipulation and Information Warfare

In analyzing Russian cyber doctrine, one must understand that neither the word “cyber” nor the term “hybrid warfare” exist independently in the Russian conceptual framework; instead,

they are used almost exclusively in reference to Western activities.⁶ While the US military has established an understanding of cyberspace as a discrete domain of warfare that deserves its own doctrine, its own troops, and its own unique menu of lethal and nonlethal effects, Russia treats cyberspace as a subordinate component to its holistic doctrine of information warfare.⁷ Cyber operations, to the Russian mind, are regarded more broadly “as a mechanism for enabling the state to dominate the information landscape,” rather than as a narrow mechanism for the achievement of discrete effects on communication systems.⁸ This distinction is evident in the Russian use of the phrase “information security” rather than the more narrowly technical notion of “cybersecurity” that prevails in US discussion.⁹

Furthermore, the Russian conception of information warfare is also more holistic in character than the typical Western understanding. Whereas the West tends to view information as data that is transmitted and stored on networks—a data- and system-centric perspective that arose out of the information theory movement of the mid-

⁶ Giles, “Russia’s ‘New’ Tools for Confronting the West.”

⁷ Medvedev, “Military Doctrine of the Russian Federation”; Giles, “Military Doctrine of the Russian Federation 2010.”

⁸ Connell and Vogler, “Russia’s Approach to Cyber Warfare.”

⁹ Thomas, “Information Security Thinking.”

twentieth century—other conceptions see information as a platform for shaping individual and collective perception, to alter how people make decisions and how societies see the world.¹⁰ The Russian conception of information warfare reflects this second, more psychological tone. Shaped by a history of confrontation with adversaries who were technologically and economically superior, the Russian military tradition depended on achieving victory through a qualitative, near-spiritual sense of moral superiority.¹¹ This moral superiority required the deliberate cultivation of a sense of psychological and cultural integrity that was strong enough to withstand the effects of outside influence. Furthermore, the imperatives of Soviet authoritarianism depended on the tight control of information flows to prevent the population from mobilizing against state power.¹²

The Russian approach to the Internet today is in many ways a natural evolution of this cultural legacy. Unlike the US cyber security framework, which has been overwhelmingly

concerned with threats to the hardware and software of the Internet rather than threats to the psyche of users, the Russian information security doctrine treats information-psychological and information-technical threats with equal severity.¹³ The 2016 version of this doctrine, for example, describes the threat of an “informational pressure” that has “the aim of diluting traditional Russian spiritual-moral values.”¹⁴ The consistent language of the past three iterations of this doctrine suggest that Russia is just as concerned with maintaining psychological, perceptual, and cultural integrity as it is with the physical state of networks or their resident data.

Noticeably absent from these discussions on cyber conflict is any mention of the role of the offense in cyberspace, something that US and British governments have far more openly discussed. There are several possible motivations for this absence, not the least of which concerns the legitimate desire to keep offensive capabilities secret. An

¹⁰ Lawson, “Russia Gets a New Information Security Doctrine.”

¹¹ Adamsky, *Culture of Military Innovation*.

¹² Soldatov and Borogan, *Red Web*.

¹³ Thomas, “Information Security Thinking.”

¹⁴ Galperovich, “Putin Signs New Information Security Doctrine.” The new information security doctrine is of the same spirit as both the 2000 and 2010 versions, the former of which includes as threats, “the devaluation of spiritual values, the propaganda of examples of mass culture which are based on the cult of violence, and on spiritual and moral values which run counter to the values accepted in Russian society.” Quote taken from Giles, “Information Troops.”

equally plausible reason is that rigid delineations between offense and defense are both difficult to establish and logically unnecessary in a cyberspace doctrine that is more psychologically than technically oriented. A 2007 article in *Moscow Military Thought* reinforces this idea: “In our view, isolating cyber terrorism and cyber crime from the general context of international information security is, in a sense, artificial and unsupported by any objective necessity.”¹⁵ By wrapping conventional notions of cybersecurity into an idea of information security that is broader and more psychologically defensive, Russia creates the conceptual space to stretch the boundaries between offensive and defensive activity—as we have seen in numerous Russian disinformation campaigns.

Understanding Russia’s psychological approach to information warfare—and further understanding its information warfare approach to cyberspace operations—allows one to evaluate the 2008 cyberattacks in their proper context. A distinguishing characteristic of psychological warfare concerns its tendency to target populations rather than militaries, a

characteristic that was reflected in the Russia-Georgia War. The specific targets selected for the campaign isolated the Georgian government from its most effective means of strategic communication and, in the process, rendered it unable to communicate with either its own population or with the outside world. Russia then filled the void created by this information blockade with a concerted propaganda campaign that allowed it to saturate the news media with its own version of events.¹⁶ Furthermore, while analysts agree that Russian hackers had the expertise to create lasting physical effects on Georgian infrastructure, their avoidance of doing so reinforces the idea that psychological manipulation and narrative control was a more important long-term purpose than any structural or service degradation the hackers may have been able to create.¹⁷ The significant amount of time that Russian hackers spent discussing the merits and drawbacks of different kinds of malware further suggests an understanding of the campaign’s higher strategic needs.¹⁸ It is worth noting, however, that the technical success of the cyberattacks was not matched by a success with the strategic

¹⁵ Giles, “Information Troops.”

¹⁶ Deibert, “Cyclones in Cyberspace.”

¹⁷ Bumgarner and Borg, *Overview by the US-CCU*.

¹⁸ *Russia-Georgia Cyber War—Findings and Analysis*.

narrative, as the Russians failed to gain international consensus around their version of events. Lessons learned from this failure led directly to Russian success in Ukraine six years later.¹⁹

In cyberspace as in physical space, it is crucial to avoid interpreting the actions of an adversary from the lens of one's own doctrine. Russian behavior in cyberspace in Georgia and beyond must therefore be evaluated within the context of Russia's conceptual orientation to the cyberspace domain. This orientation manifests itself in an information security doctrine that is preoccupied with a sense of both physical and psychological vulnerability and that, therefore, implicitly grants societal targets the same legitimacy as military ones. As a result, the Russian perspective on cyberspace views deception, manipulation, and denial as legitimate tools of statecraft that today's mass communication platforms readily enable. Actions that we would characterize as discrete, technical, and fundamentally offensive in character—such as DDoS and website defacement—instead reflect Russia's holistic approach to cyberspace as a tool of

information warfare rather than as a fundamentally separate war-fighting domain.²⁰ The 2008 Russia-Georgia War was the first overt test of this approach in a conventional military context; in the decades since, it has been implemented with increasing refinement both inside and outside the post-Soviet sphere and both inside and outside a conventional military setting.²¹



Cyberattacks in the Russia-Georgia War Highlight the Increasing Relevance of Third Forces to Future Conflict

The cyberattacks of the Russia-Georgia War provide empirical evidence of the extent to which cyberspace empowers third-party non-state actors in modern conflict. The US Army Strategic Studies Institute categorizes these actors as “third forces,” or “organizations that can influence the outcome of armed conflict

¹⁹ Giles, “Information Troops.” This idea of Georgia as a warm-up for Ukraine, in physical and in informational space, was also reinforced during author interviews in Georgia.

²⁰ Russia has employed many of these same information-warfare tools against domestic audiences, as Soldatov and Borogan describe in *The Red Web*.

²¹ Since 2008, Russian has conducted cyber operations and information operations in conjunction with a military campaign in Ukraine and Syria and absent a military campaign in Finland, Latvia, France, Germany, and the United States.

but are not, strictly speaking, combatants.”²² The Russia-Georgia War provides several examples of how third forces can exert influence on the battlefield both inside and outside state control. The first such example is the Russian hackers themselves. Russia has a well-documented history of employing civilians, criminal syndicates, and armies of social media bots²³ to rapidly increase the depth and breadth of its offensive cyber footprint with minimal levels of state attribution.²⁴ In this tradition, the cyberattacks in Georgia were not perpetrated by a uniformed arm of the Russian state, but by patriotic citizens who were engaged and recruited through social media. The primary hacker forums for coordination and tool dissemination were [xaker.ru](#) and [StopGeorgia.ru](#). The hacker communities within them followed a distinct hierarchy in which the more technically skilled forum leaders provided the tools, vulnerabilities, and target lists for the less tech-savvy followers to action.²⁵

Russian political culture has two attributes that make it particularly adept at marshaling these non-state cyber resources in the service of its strategic goals, a process that Alexander Klimburg calls “mobilizing cyber power.”²⁶ The first is a historically cozy relationship between the state and organized crime. In cyberspace this relationship is most evident in the nefarious online activity of the Russian Business Network (RBN), which is the only criminal organization identified by NATO as a major strategic threat.²⁷ ShadowServer Foundation identified at least six different C2 servers used in the conflict, all of which had a preexisting record of DDoS activity.²⁸ Some of the zombie computers involved even conducted attacks on unrelated e-commerce websites amidst the Georgia campaign.²⁹ The second attribute that enables Russian recruitment of its patriotic hacker community is a long-standing political tradition of propaganda, agitation, and narrative control designed to shape the collective psyche and mobilize the popular consciousness in service of the state. This

²² *US Army War College Key Strategic Issues List 2016–2017*.

²³ Chen, “Agency.”

²⁴ Klimburg, “Mobilising Cyber Power.” See also Soldatov and Borogan, *Red Web*, for examples of domestic use.

²⁵ *Russia-Georgia Cyber War—Findings and Analysis*.

²⁶ Klimburg, “Mobilising Cyber Power.”

²⁷ *Ibid.*

²⁸ Deibert, “Cyclones in Cyberspace.”

²⁹ Bumgarner and Borg, *Overview by the US-CCU*.

tradition led to the creation of several Kremlin-sponsored youth movements in the mid-2000s, which have since been implicated in both trolling and DDoS operations against Kremlin opponents.³⁰ Accordingly, the first step of the kill chain for the Georgia cyberattacks entailed an encouragement of novices “through patriotic imagery and rhetoric to get involved in the cyber war against Georgia.”³¹

While Russia claims that it neither supports nor encourages these cyber privateers, internal military discourse indicates that the Russian state is well aware of the strategic advantages they provide. Following the 2008 campaign, discussion within the Russian military cited a poor performance in the information domain as evidence of the need for “Information Troops” within the Russian armed forces who were capable of conducting full-spectrum information operations.³² Criticisms of this proposal stemmed from a reluctance to cede the many benefits of the existing arrangement. First, the use of citizen hackers allows Russia to circumvent one of the greatest challenges in cyberspace: recruiting and retaining talent. The execution of effective cyberspace operations

requires a level of creativity and innovation that disciplined, hierarchical, and process-oriented militaries find difficult to accommodate. Recognizing that military organizations are ill situated to cultivating talent, the best coders often head to the private sector, leaving militaries with a crisis in manpower even as the requirements for effective cyber defense and offense increase.³³ A reliance on third-party actors allows a state to capitalize on the richest talent pools without having to significantly overhaul their entrenched military processes. These private-sector actors, unburdened by the rigid hierarchies of authority that rightfully safeguard the military application of lethal violence, are far more proficient in the type of operational agility that cyberspace requires. This agility was evident in the chronology of the Russia-Georgia War, as the Russian hackers were able to effectively counter each successive Georgian response, through rapidly executed actions of increasing technical sophistication.

Furthermore, the use of non-state hackers allows the Russian state to elude formal attribution from the hackers’ cyber activities. Since attribution is a precondition for

³⁰ Soldatov and Borogan identify two groups in particular: Nashi (“Ours”) and Molodaya Gvardiya (“Young Guard”), the latter of which created its own media wing in 2013 to help with domestic Internet censorship.

³¹ *Russia-Georgia Cyber War*.

³² Giles, “Information Troops.”

³³ Evans and Reeder, *Human Capital Crisis in Cyber Security*; “US Army Introduces Cyber Fast Track for Civilians”; *Borderless Battle*.

retaliation, the use of non-state hackers enables a state to inhabit an operational gray space that complicates the pursuit of a response and obfuscates the applicability of international law.³⁴ To this day, there exists no forensic evidence that definitively connects the Russian government to cyber actions against Georgia. Referencing the effectiveness of the citizen-led Georgian campaign, one report stated outright that “there is no need for the state machine in modern cyber warfare.”³⁵ In the Russian calculus, the use of non-state hackers offers a set of utilitarian advantages that outweighs any associated reputational costs: citizen hackers are anonymous, they can be mobilized quickly, they require no additional state training, and they are operationally agile. While Russia has recently signaled an intention to bolster the cyber capability of its armed forces, the aforementioned advantages suggest that its reliance on third-party actors to execute the state’s cyber operational dirty work is unlikely to go away as an auxiliary tactic any time soon.³⁶

Acknowledging the role of unregulated

third-party actors in cyber conflict also requires us to contend with the patriotic amateur hacking wars that such actors will inevitably incite. Because amateur hackers are not bound by the same considerations of collateral damage that restrict military cyberspace operations, their potential involvement in future conflict is a concerning development. One of the first elements of Georgian society that was deliberately attacked was a hacking forum called www.hacking.ge, an effort to forestall a Georgian counterattack by neutralizing its citizen hacking community.³⁷ This action precipitated limited Georgian attacks against Russian websites, thereby resulting in an independent cyber conflict between non-state actors under the cover of officially declared state hostilities.³⁸ Furthermore, while the nationality of the hackers remained relatively evenly distributed among pro-Russian and pro-Georgian sympathizers, the infrastructure that they fought with touched over sixty different sovereign countries, suggesting that the digital repercussions of future conflict will extend far beyond the physical boundaries of the military

³⁴ Tikk et al., *Cyber Attacks against Georgia*.

³⁵ Giles, “Information Troops.”

³⁶ Connell and Vogler, “Russia’s Approach to Cyber Warfare.”

³⁷ Tikk et al., *Cyber Attacks against Georgia*.

³⁸ Other noteworthy examples of patriotic hacking wars include Kosovo in 1999, the Second Intifada in 1999, digital skirmishes between India and Pakistan in 2000, and the Hainan Island Incident in 2001.

actions that inspired them.³⁹

The multinational nature of the 2008 Russian cyber campaign raised a variety of legal issues that will accompany any use of third forces on the cyber battlefield. First, the use of citizen hackers and other non-state parties complicates the selection of an appropriate legal framework to govern the international response. As the Cooperative Cyber Defense Center of Excellence (CCD COE) articulates, the fact that physical hostilities might meet the standard for application of the law of armed conflict (LOAC)—defined as “any difference arising between two states and leading to the intervention of armed forces”—does not mean that cyber hostilities will also. On the contrary, both the Council of Europe (COE) convention and current US law still formally view the July 2008 DDoS attack against Georgia as a cyber crime.⁴⁰ Absent LOAC, a state must default to either criminal law or information and communications (ICT) regulation. While Estonia benefited from a more well-developed ICT legal framework that helped to guide its response to Russian cyberattack in 2007, Georgia did not have the benefit of anything comparable in its domestic law. An additional legal complication concerned formal state attribution. In international law, it

is assumed that the conduct of a private actor is not attributable to the state unless the state has “directly and explicitly delegated a part of its tasks and functions to a private entity.”⁴¹ As numerous reports have verified, this level of control remains unproven in the case of the Russia-Georgia War. Reliance on private cyber militias therefore offers a level of plausible deniability to states who wish to further complicate the response options that are legally available to an adversary.

The Russia-Georgia conflict introduced another type of third-party actor—the private tech companies that own contested cyber terrain. On August 8 the owner of Tulip Systems (TSHost), a private web-hosting company in Atlanta, contacted the president of Georgia to offer assistance in reconstituting their Internet capabilities. On August 9 the Georgian government transferred critical Internet capabilities to TSHost servers in the United States, including the websites of the Ministry of Defense and the president. Undeterred, the cyber attackers brought their DDoS capabilities to bear on American targets. The significance of this move cannot be overstated: an American company, with no authority and no clear US approval, brought a conflict to the

³⁹ Deibert, “Cyclones in Cyberspace.”

⁴⁰ Korns and Kastenber, “Georgia’s Cyber Left Hook.”

⁴¹ Tikk et al., *Cyber Attacks against Georgia*.

shores of a neutral sovereign state by negotiating directly with a foreign government. Had the cyberattacks been considered an act of war rather than an act of international crime, the unilateral relocation of Georgian cyber infrastructure to the United States could have violated Hague (V) article 3, which forbids belligerents from erecting on the territory of a neutral power a “wireless telegraphy station or other apparatus” for the purpose of communicating with belligerent forces.⁴²

Theories of warfare, in physical space or otherwise, tend to presuppose an ecosystem of exclusively government actors. Cyberspace challenges this presupposition, since the domain, the expertise to succeed in it, and its most sophisticated operational innovations have evolved largely outside of either state or military control. The interconnected nature of the domain has caused private actors to become increasingly entangled with the affairs of state, and state actors to become increasingly powerless in the face of expanding threats.⁴³ As

Jason Healy states in his comprehensive history of cyberspace, the primacy of the private sector in resolving conflict is one of the crucial distinguishing features between cyber and traditional conflicts.⁴⁴ The Russia-Georgia War provides an excellent, early example of the implications of such public-private entanglement, from patriotic citizen hackers who engage in their own private war to independent cybersecurity firms who engage in their own private diplomacy. By demonstrating many of the ways in which cyberspace enables these so-called third forces, this conflict foreshadowed many of the challenges and critical questions of conflicts to come.⁴⁵



⁴² Korns and Kastenber, “Georgia’s Cyber Left Hook.”

⁴³ *Borderless Battle*. See also current congressional testimony on the role of Twitter, Google, and Facebook in the 2016 US elections.

⁴⁴ Healy, *Fierce Domain*.

⁴⁵ Later examples of this new private-public dynamic include Stuxnet, in which the independent discoveries of three private cybersecurity firms unintentionally derailed the most sophisticated cyber sabotage program in history (see Zetter, *Countdown to Zero Day*); cybersecurity firm Mandiant (now FireEye), whose 2013 report on APT 1 allowed the US government to further the Chinese dialogue without having to disclose classified sources and methods; and Google Jigsaw, which addresses problems of societal security through technological solutions enacted almost entirely on Google’s own platforms. For example, Google Jigsaw’s ongoing counterextremist campaign redirects potential ISIS recruits toward more-moderate material.

Cyberattacks in the Russia-Georgia War Show That Cyberspace Can Be Understood through, and Employed with, Existing Operational Principles

A significant obstacle to planning for and integrating cyber effects into conventional military operations is the inability of the technical and nontechnical communities to understand one another, a phenomenon that Jason Healy describes as a “mutual misunderstanding between the ‘geeks’ and the ‘wonks.’”⁴⁶ Those with the operational insight to recognize effective requirements for a campaign plan usually lack the specific technical knowledge to articulate how those requirements might be supported, while those with the technical knowledge to create solutions often lack adequate access to the planning process or adequate understanding

of the larger strategic picture. Both sides are often stifled by poor communication channels and unaccommodating legal authorities. The resultant lack of demonstrated cyberspace effectiveness only further disinclines the supported community from requesting cyber effects in the future, thus perpetuating a cycle of missed opportunities for successful cyberspace integration that inhibits further capability development. Integration efforts are further stifled by the perception that cyberspace is new and different, when one could argue that there are clear historical analogues both for its effects⁴⁷ and its integration.⁴⁸

This gap in understanding is based in large part on the erroneous notion that cyberspace is too technical and too unique for the traditional war-fighting community to grasp. While the Army has made an effort to

⁴⁶ Healy, *Fierce Domain*, 16.

⁴⁷ Electronic warfare, signals intelligence, and information operations all possess similarities to the cyberspace operations of today. As Michael Warner argues in his “Cybersecurity: A Prehistory,” current cyberspace doctrine bears a strong resemblance to concepts of information warfare in the early 1990s.

⁴⁸ While the analogy that the US military is “building an airplane while in flight” in respect to cyberspace operations is woefully overused, there are important parallels to be drawn between the creation of air doctrine in the interwar years and the creation of cyber doctrine today. The Germans, the Americans, and the Brits all came to different conclusions as to how air power should be used, each of which failed to prove holistically effective when the motivating strategic circumstances were upturned. Several of the factors that went into these conclusions are present in some degree today: interservice rivalries and the consequent jostling for resources; the influence of technologies developed (or not) in the civilian sector; the multiple perspectives on the nature of the threat and of future war; the influence of personnel background on the thinking of each country’s new air organizations; and most importantly, the set of assumptions that underpinned each service’s estimation of the validity of their doctrinal projections. See Murray and Millett, *Military Innovation in the Interwar Period*, for a more detailed account of this and other examples of differing approaches to the same technology.

rectify this conceptual discrepancy through the integration of 131A targeting warrants into its cyber formations and through tactical outreach initiatives such as Cyber Support to Corps and Below (CSCB), developing a shared understanding of cyberspace operations remains an institutional challenge throughout the broader force. The author is intimately familiar with the American experience in this regard, but Russian military discourse suggests that they also face similar challenges.⁴⁹ Generating an understanding of cyberspace outside the cyberspace community (and in some cases inside it as well) is therefore critical to the successful implementation of cyberspace capabilities on a large scale. The Russia-Georgia conflict offers several important lessons in this regard.

In offering the first publicly available evidence that large-scale, overt cyberattacks can be effectively nested with and understood through the lens of a maneuver campaign, the Georgian war represents a critical opportunity to bridge the conceptual gap that currently stifles the art of the possible in planning for effective cyberspace operations. First, the war demonstrated that cyber effects must pursue the same strategic, operational, and tactical purpose as the maneuver campaign they support. One of Russia's primary strategic

objectives in Georgia was to reassert its power in the former Soviet periphery. Russian strength had to be contrasted with Georgian impotence, and so the Georgian government itself became the center of gravity for both the cyber campaign and the physical campaign. Cyberattacks enabled this purpose by demonstrating the Georgian government's tenuous authority in digital space while Russian conventional forces demonstrated the same in physical space. Furthermore, by targeting only those sites whose loss would pose an inconvenience rather than those that would cause chaos or injury, Russian hackers demonstrated a level of restraint in their target selection that nested with the strategic need to avoid overly provoking the international community.

The Russia-Georgia War also helped to debunk the "speed of cyber" fallacy. This fallacy centers on a myth that everything in cyberspace happens instantaneously, creating a sense of temporal misunderstanding that complicates effective cyber planning. It is true that cyberattacks can unfold more rapidly than attacks in physical space, since the digital domain is unencumbered by the limitations of terrain, logistics, or human endurance. However, because cyberattacks are dependent on a long process of identifying vulnerabilities,

⁴⁹ Giles, "Information Troops."

developing exploits against those vulnerabilities, and then maintaining access to the targets that have them, a successful cyber campaign still requires months, if not years, of preparation and planning. Furthermore, a trained cyber force requires human capital supported by doctrine, training, technology, command and control, and physical infrastructure. As Dave Hollis states, one “cannot engage in cyber war from a cold start.”⁵⁰ In cyberspace, as in physical space, the speed of a campaign’s execution is often inversely related to the amount of time spent preparing to carry it out.

That Russian hackers were able to immediately engage in website defacement and denial of service attacks at the outbreak of hostilities in Georgia reveals the extent to which they had prepared for such hostilities beforehand. As the US-CCU reports, one of the tools used for website defacement had been created over two years prior, specifically for a campaign against Georgia. Many of the subordinate domains to StopGeorgia.ru had been registered several months before the outbreak of hostilities, and the hosting company used to register the site had been reported by malware-monitoring sites nearly two months prior to the conflict.⁵¹ The

extensive preparation required in advance of cyber conflict allows for the assessment of synchronized cyberspace actions as an intelligence indicator for follow-on military operations. In the case of Georgia, these indicators took several forms and appeared at several different stages of the operational cycle: chat rooms in which hackers were recruited during the force-mobilization process; reconnaissance of digital targets to identify exploitable vulnerabilities; attacks against rival hacker communities as a preemptive strike on the adversary’s rear; and the neutralization of news sites prior to physical attack could all be seen, retrospectively, as mounting evidence of an armed campaign. Systematically identifying when, why, and how each of these indicators appears in adversary behavioral patterns can help improve how we integrate both offensive and defensive cyber capabilities into conventional operational processes.

Additionally, while the specific tactical language of cyberspace may differ from that of maneuver, the Georgian campaign demonstrated that many of the same general principles still apply. An acknowledgment of this fact is important in helping to reframe how we consider and communicate cyberspace

⁵⁰ Hollis, “Cyberwar Case Study.”

⁵¹ Carr, *Inside Cyber Warfare*.

operations in a conventional kinetic context. For example, a technical explanation of SQL injection, blind SQL injection, and the use of Benchmark to maximize expended processing power—techniques that were all used in 2008—could be reconceived for a different audience as a discussion of creating massing effects while maintaining economy of force. The command and control principles behind a DDoS attack could be further understood as an example of centralized command and decentralized execution, with numerous command and control centers that enable unity of effort across an otherwise invisible cyberspace army.

Existing doctrinal language and principles are equally relevant to the demystification of the cyber defense. Estonia, having a comparatively robust ICT infrastructure with stronger regulatory and legal frameworks to govern it than what existed in Georgia, was able to defend in place—albeit with limited success—against a much larger attacking force. Georgia, on the other hand, with a physical and legal ICT infrastructure that was poorly developed in comparison, had to employ a mobile defense in which it shifted website hosting to alternate battle positions—in this case, other countries that had more available bandwidth and greater filtering

capacity. Georgian hackers then attempted a twofold response that was met with limited effect. After first blocking Russian IP addresses and known attack protocols, they attempted a counterattack against select Russian websites. In response, Russian hackers employed IP spoofing to mask the source location of their attacks and changed elements of their attack protocols. While this response is rather prosaic from a technical perspective, it encapsulates the maneuver doctrinal pattern of action, reaction, counteraction; and as such, it can be understood from a maneuver standpoint as an example of classic Soviet operational art—“attacking with operations from multiple directions so that the enemy is faced with overwhelming challenges on where to concentrate its effort.”⁵² Cultivating an understanding of cyber defense according to maneuver principles could greatly improve the ability of fighting organizations to defend themselves, as it renders otherwise unintelligible technical terminology into a more broadly accessible format.

The final theme we see in the Georgian cyberattacks is that terrain in cyberspace matters. One of the many fallacies about cyberspace, and one that feeds the systemic hyperbole around discussions of cyberwar, is that cyberspace has no geography. As the

⁵² Donovan, “Russian Operational Art in the Russo-Georgian War of 2008.”

analysis in the preceding section shows, however, geography played a significant role in the effectiveness of cyberattacks in Georgia. US doctrine defines cyberspace in terms of three layers: physical, logical, and cyber persona.⁵³ While a great deal of malleability exists at the logical layer, allowing users to create, modify, and destroy cyber terrain in a way that has no physical analogue, cyberspace operations still have to contend with realities at the physical layer that no amount of software can overcome. For example, the fact that Estonia possessed its own Internet exchange point (IXP) in 2007 allowed it to cut off the brunt of malicious Russian traffic without hindering its ability to communicate internally. Absent this critical piece of Internet geography, Georgia lacked the ability to defend against international attacks without simultaneously sabotaging their own domestic capabilities.⁵⁴

Furthermore, the physical reality of cyberspace is the first point of reference for determining jurisdiction and the application of authorities; as a result, it is also where the global nature of cyberspace can quickly run into geopolitical issues of sovereignty, as demonstrated in the decision by Tulip Systems

to host Georgian networks on US servers. The geography of cyberspace in the Russia-Georgia War meant that Russia was able to effectively isolate Georgia from the global Internet by targeting a few vulnerable choke points of cyber terrain. Georgia's physical dependence on Russian network infrastructure, with nearly half of Georgian network routes passing through Russia, amplified the effectiveness of the Russian cyberattacks.⁵⁵ This reality demonstrates that terrain dictates the plan in cyberspace no differently than it does in conventional maneuver and can once again help to focus the often-chaotic nature of cyberspace planning.⁵⁶

As the first publicly available example of a coordinated cyberattack employed in concert with a conventional military campaign, the Russia-Georgia War demonstrated that cyberspace operations can be employed with and understood through the same maneuver principles that it supports. It therefore serves as a useful template for addressing the critical conceptual gap between the technical and nontechnical planning communities that continues to challenge the effectiveness of cyberspace operations nearly a decade later.

⁵³ Joint Chiefs of Staff, *Cyberspace Operations*.

⁵⁴ Healy, *Fierce Domain*, 72.

⁵⁵ Russell, "Georgia-Russia War."

⁵⁶ Raymond et al., "Key Terrain in Cyberspace."

However, such a realization carries with it several cautions. First, while cultivating an understanding of cyberspace through the lens of maneuver principles serves the necessary purpose of demystifying an otherwise-abstruse domain, in itself this effort is insufficient for creating the type of detailed technical understanding that is necessary for cyberspace operations personnel. Second, this effort should not be pursued at the exclusion of the type of deep strategic thinking required to fully realize the domain's military and grand strategic potential. For example, one of the more revolutionary aspects of cyberspace is the extent to which it promotes a near-constant state of low-level conflict, one that equally defies our traditional understandings of war and our traditional frameworks for strategy.⁵⁷ As we attempt to integrate new technology into existing doctrine, we would be wise to embark on the critical venture of questioning which aspects of our doctrine deserve to be reconsidered. Historical experience offers ample evidence of the perils that befall those militaries that fail to adequately question their own doctrinal assumptions as they pursue the

development and implementation of new technologies of war.



Conclusion

Methods of cyberattack have evolved in sophistication and complexity since their first overt integration with large-scale ground maneuver in the 2008 Russia-Georgia War. However, while technologies have changed in the past decade, the underlying dynamics of cyber conflict have not. This paper has attempted to highlight three of the more enduring lessons learned from the conflict that remain applicable to scholarly and military pursuits.

First, the 2008 cyber campaign reinforces the Russian conception of cyberspace as a tool for information warfare rather than as a discrete, effects-based war-fighting domain. This conception has inspired increasingly assertive efforts to pursue Russian strategic

⁵⁷ For examples of the discussion over the extent to which cyberspace is unique, see Rid, "Cyber War Will Not Take Place"; Stone, "Cyber War Will Take Place!"; Gartzke, "Myth of Cyberwar"; Lee and Rid, "OMG Cyber!"; Junio, "How Probably Is Cyber War?"; Lawson, "Beyond Cyber Doom"; Lindsay, "Stuxnet and the Limits of Cyber Warfare"; Haggard and Lindsay, "North Korea and the Sony Hack." Further discussions concern cyberspace's role in deterrence, a framework that was inherited from the nuclear age and whose fundamental precepts only questionably apply to the cyber domain. See Glaser, *Deterrence of Cyber Attacks and US National Security*; Rid and Buchanan, "Attributing Cyber Attacks"; Lindsay and Gartzke, "Coercion through Cyberspace"; Buchanan, *Cybersecurity Dilemma*; Nye, "Deterrence and Dissuasion in Cyberspace."

objectives through digital means, to include the 2016 and 2017 targeting of US and European democratic elections. Turning our scholarly sights toward Russian information-warfare doctrine, as well as its Soviet doctrinal predecessors, will better prepare us to contend with those uses of cyberspace that do not fit neatly into our own doctrinal framework and that do not present as cleanly defined offensive acts.

Second, the 2008 Georgian cyberattacks demonstrated the increasing influence of third forces to the modern battlefield. As such, they exemplify the diffusion of power phenomenon that takes the mechanisms of conflict beyond state control. The influence of these actors on the cyber battlefield both complicates the direct application of the laws of armed conflict and affects the range of state action available for response, since private actors own the majority of cyberspace infrastructure. Efforts are underway to more effectively harness the power of the private sector in pursuit of holistic cybersecurity,⁵⁸ but a great deal of research remains in understanding the implications of these actors to modern conflict.

Finally, the conflict demonstrated that cyberspace operations can be effectively leveraged with and understood through traditional operational principles—an insight of evolutionary utility that should not preclude the embrace of cyberspace’s revolutionary qualities. Military professionals must be as comfortable speaking about cyberspace operations as they are those on land, in air, or at sea if we are to fight effectively moving forward. The Russia-Georgia conflict offers one possible interpretation of how to merge these different war-fighting vocabularies.

Success in war depends not on simply discovering a new technology but on discovering the best way to use it. Thus, the effective operational integration of cyberspace with conventional military activity is contingent on the effective conceptual integration of cyberspace operations with how we envision future war. While a great deal of deep, doctrinal thinking remains to be accomplished in creating that holistic vision, our efforts would be well served by looking toward the lessons of past cyber conflicts to inform how we approach the future.

⁵⁸ *Borderless Battle*.

Bibliography

- Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel*. Palo Alto, CA: Stanford University Press, 2010.
- Borderless Battle: Defending against Cyber Threats; Hearing before the Committee on Homeland Security, House of Representatives*. 115th Cong., 1st Sess. March 22, 2017. <https://www.hsdl.org/?view&did=800990>.
- Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. New York: Oxford University Press, 2016.
- Bumgarner, John, and Scott Borg. *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*. Special report. US Cyber Consequences Unit, 2009.
- Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastapol, CA: O'Reilly Media, 2010.
- Chen, Adrian. "The Agency." *New York Times*, June 2, 2015. <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>.
- Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." CNA's Occasional Paper series, CNA, Arlington, VA, March 2017, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.
- Deibert, Ronald J. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War." *Security Dialogue* 43, no. 1 (2012): 3–24.
- Donovan, George T. "Russian Operational Art in the Russo-Georgian War of 2008." Strategy Research Project, US Army War College, Carlisle, PA, 2009.
- Dorell, Oren. "Russia Engineered Election Hacks and Meddling in Europe." *USA Today*, January 9, 2017. <https://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/>.
- Evans, Karen, and Franklin Reeder. *A Human Capital Crisis in Cyber Security: Technical Proficiency Matters*. Washington, DC: Center for Strategic and International Studies, Commission on Cybersecurity, 2010. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/101111_Evans_HumanCapital_Web.pdf.
- Fanelli, Robert L. "Cyberspace Offense and Defense." *Journal of Information Warfare* 15, no. 2 (2016): 53–65.
- Freedburg, Sydney J., Jr. "Russia's Information War: Latvian Ambassador, Finnish Strategist Warn on Cyber." *Breaking Defense*, June 6, 2014. <https://breakingdefense.com/2014/06/russias-information-war-latvian-ambassador-finnish-strategist-warn-on-cyber/>.

- Galperovich, Danila. "Putin Signs New Information Security Doctrine." *Voice of America News*, December 8, 2016. <http://www.voanews.com/a/russia-new-information-security-doctrine/3628197.html>.
- Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security Studies* 38 no. 2 (2012): 41–73.
- Giles, Keir. "Information Troops: A Russian Cyber Command?" In *3rd International Conference on Cyber Conflict*, edited by C. Czosseck, E. Tyugu, and T. Wingfield. Tallin, Estonia: CCD COE Publications, 2011.
- . "The Military Doctrine of the Russian Federation 2010." NATO Research Review, NATO Defense College, Rome, February 2010, http://www.conflictstudies.org.uk/files/MilitaryDoctrine_RF_2010.pdf.
- . "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power." Chatham House: The Royal Institute for International Affairs, London, March 2016, <https://www.chathamhouse.org/publication/russias-new-tools-confronting-west>.
- Glaser, Charles L. *Deterrence of Cyber Attacks and US National Security*. Washington, DC: Cyber Security Policy Research Institute, George Washington University, 2011.
- Haggard, Stephan, and Jon R. Lindsay. "North Korea and the Sony Hack: Exporting Instability through Cyberspace." AsiaPacific Issues paper, no. 117, Analysis from the East-West Center, Honolulu, HI, May 2015).
- Healy, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. London: Carbon Capture and Storage Association, 2013.
- Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, January 6, 2011. <http://smallwarsjournal.com/print/10080>.
- Intelligence Community Assessment. *Assessing Russian Activities and Intentions in Recent US Elections*, ICA2017-01D, January 6, 2017. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
- Joint Chiefs of Staff. *Cyberspace Operations*, Joint Publication 3-12 (R), February 5, 2013. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf.
- Junio, Timothy J. "How Probable Is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate." *Journal of Strategic Studies* 36, no. 1 (2013): 125–33.
- Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. New York: Simon and Schuster, 2016.
- Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011): 41–60.
- Korns, Stephen W., and Joshua E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters* 38, no. 4 (2009): 60–76.

- Lawson, Sean. "Russia Gets a New Information Security Doctrine." *Forbes*, December 9, 2016. <https://www.forbes.com/sites/seanlawson/2016/12/09/russia-gets-a-new-information-security-doctrine/#503b640f3fc4>.
- . "Beyond Cyber Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber Threats." *Journal of Information Technology and Politics* 10, no. 1 (2013): 86–103.
- Lee, Robert M., and Thomas Rid. "OMG Cyber!" *RUSI Journal* 159, no. 5 (2014): 4–12.
- Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365–404.
- Lindsay, Jon R., and Erik Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." In *The Power to Hurt: Coercion in Theory and Practice*, edited by Kelly M. Greenhill and Peter J. P. Krause, 179–203. New York: Oxford University Press, 2016.
- Medvedev, Dmitry. "Military Doctrine of the Russian Federation." Originally published on the President of the Russian Federation website. February 5, 2010. Translated by Carnegie Endowment for International Peace. http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.
- Murray, Williamson, and Allan R. Millett, eds. *Military Innovation in the Interwar Period*. New York: Cambridge University Press, 1996.
- Nye, Joseph S., Jr. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (2016): 44–71.
- Raymond, David, Tom Cross, Gregory Conti, and Michael Nowatkowski. "Key Terrain in Cyberspace: Seeking the High Ground." In *2014 6th International Conference on Cyber Conflict: Proceedings*, edited by P. Brangetto, M. Maybaum, and J. Stinissen, 287–302. Tallinn, Estonia: NATO CCD COE Publications, 2014.
- Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.
- Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, nos. 1–2 (2015): 4–37.
- Russell, Alison Lawlor. "The Georgia-Russia War." In *Cyber Blockades*. Washington, DC: Georgetown University Press, 2014.
- Russia-Georgia Cyber War—Findings and Analysis*. Phase I Report. Project Grey Goose, October 17, 2008. <https://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>.
- Segal, Adam. *Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2016.
- Soldatov, Andrei, and Irina Borogan. *The Red Web*. New York: PublicAffairs, 2015.
- Standish, Reid. "Why Is Finland Able to Fend Off Putin's Information War?" *Foreign Policy*, March 1, 2017. <http://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/>.

- Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (2013): 101–8.
- Thomas, Timothy L. "Information Security Thinking: A Comparison of US, Russian, and Chinese Concepts." In *International Seminar on Nuclear War and Planetary Emergencies—26th Session*, edited by R. Ragaini, 344–56. River Edge, NJ: World Scientific Publishing, 2002.
- Tikk, Eneken, Kadri Kaska, Kristel Rünnermeri, Mari Kert, Anna-Maria Taliarm, Liis Vihul. *Cyber Attacks against Georgia: Legal Lessons Identified*. Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2008.
- Tucker, Patrick. "The Sarin Gas Attack in Syria Ignited an Information Battle." *Defense One*, April 6, 2017. [http://www.defenseone.com/technology/2017/04/sarin-gas-attack-syria-ignited-information-battle/136819/?oref=defenseone today nl](http://www.defenseone.com/technology/2017/04/sarin-gas-attack-syria-ignited-information-battle/136819/?oref=defenseone%20today%20nl).
- "US Army Introduces Cyber Fast Track for Civilians." *Signal*, February 13, 2017. <http://www.afcea.org/content/?q=Blog-us-army-introduces-cyber-fast-track-civilians>.
- US Army War College Key Strategic Issues List 2016–2017*. Carlisle, PA: US Army War College Press, July 31, 2016. <https://ssi.armywarcollege.edu/pdffiles/PUB1334.pdf>.
- Warner, Michael. "Cybersecurity: A Prehistory." *Intelligence and National Security* 27, no. 5 (2012): 781–99.
- Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books, 2016.

