THE CYBER BATTLEFIELD

Russia has been at the vanguard of militarizing cyberspace

By **MAJ. DANIEL SINGLETON,** U.S. Army

VEER

In April 2007, the Estonian government moved a bronze statue of a Soviet soldier from a prominent place in the Tallinn city center to a military cemetery. The statue was controversial because it commemorated the "liberation" of Estonia by the Soviet Union. Ethnic Russians rioted against the decision and within a day of the statue's relocation, Russian-language websites began calling for armed revolution. During the next few weeks, the situation escalated. Massive cyber attacks originating from Russian servers were launched against Estonia's government and civilian infrastructure. These were mostly distributed denial of service (DDoS) attacks that clog Internet servers and render them inaccessible but do no permanent damage. Because Estonia is probably the most "wired" country in the world, the attacks impacted nearly every area of life and business. And these were relatively simple attacks.

Former U.S. counterterrorism chief Richard Clarke suggests in his book *Cyber War* that China has planted logic bombs[1] in the U.S. electric grid — essentially the equivalent of "dozens of Chinese government agents running around the country strapping C4 explosive charges to those big, ugly high-tension transmission-line towers and to some of those unmanned step-down electric substation transformers that dot the landscape."[2] He argues that Chinese cyber attacks dominate the news only because the Russians are better at covering their tracks.[3]

This article is a case study of cyber war from a Russian perspective: how the Russians view it, how they wage it, and what kind of international agreements they might be open to as the world confronts the challenges of applying international law to this new form of warfare.

The West generally views "cyber war" as activity that brings about the effects ordinarily caused by war but within the framework of the Internet, intranets, and all communication networks and devices connected to them. A related but broader term is "information war," which is the fight to control information itself. However, each region uses the term differently. The West uses "war" metaphorically, in the same way we spoke of the "Cold War." Even though it is normally used in conjunction with declared hostilities and military operations, "information war" does not constitute war in and of itself. But when those in the East, including Russia, speak about information war, they literally mean war, just by nonmilitary means.[4]

Unlike information war, both East and West usually see cyber war as a form of war. It describes the use of force even if it does not use typical weapons, because it has the potential to bring about military effects. Entering a network and causing physical destruction or damage to systems is a component of cyber attack that most would recognize as the equivalent of a conventional attack. In 2010, Gen. Keith Alexander, commander of U.S. Cyber Command, affirmed America's right to respond kinetically to cyber attacks that the Pentagon determines constitute an "armed attack."[5] This principle has been dubbed "cyber equivalency" and argues for a sort of *jus ad bellum* parity in regard to the methods that may initiate a war.

Although disconcerted by Alexander's remark,[6] Russia also recognizes cyber equivalency. For example, as four Russian colonels noted in the Russian military affairs magazine, *Voennaia Mysl'*: "… the heads of the member states of the Shanghai Cooperation Organization … established that the usage of modern information technology towards military-political goals could cause global catastrophes comparable in their destructive consequences with the results caused by weapons of mass destruction."[7] Russia does not disagree with the U.S. that cyber attacks can inflict damage equivalent to kinetic attacks and may be answered by either means. When Russians draw attention to Alexander's remark, it simply illustrates their concern that their own cyber operations or those of their surrogates might be met with what they view as a disproportionate response. But the issue of war in cyberspace is far more complex.

In Russia's view, there is no global Internet. Russia's proposal for principles of Internet governance at the 2012 World Conference on International Telecommunications reads: "Member States shall have the sovereign right to establish and implement public policy, including international policy, on matters of Internet governance, and to regulate the national

Summary of Legal Positions on the
LAW OF WAR IN CYBERSPACE

Russian Federation	New international law is required to delegitimize cyber war. Current law is inadequate. Source: Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*
Collective Security Treaty Organization (CSTO)	While the CSTO has no official position, its leaders have likened cyberspace to anarchy that threatens the security of its member countries. Source: Joshua Kucera, "With Eye To Arab Spring, CSTO Strengthens Cyber, Military Powers"
European Union	Current international law should apply in cyberspace, but further dialogue and development of norms is necessary. Source: European Commission
North Atlantic Treaty Organization (NATO)	The law of war is difficult to apply in cyberspace because cyber attacks are unlikely to cause significant destruction, and the identity of the attacker is hard to determine. Source: NATO Council of Canada
United States of America	Cyber war already falls under the same laws as its kinetic counterpart. No new law is needed. Source: Elena Chernenko, "Russia warns against NATO document legitimizing cyberwars"

Internet segment, as well as the activities within their territory of operating agencies providing Internet access or carrying Internet traffic."[8] In this view, cyberspace is not an international asset, but comparable to national airspace, land or any other physical space.[9] As such, each state has sovereignty over the Internet within its borders. This broad concept of domination of the Internet by individual states is necessary for the Russian military's plans for operating within it. Col. S.I. Bazylev, et al., explains why:

> *"The activity of the Russian Federation Armed Forces in information space is mainly aimed at restraining and preventing military conflicts in information space. In practice, this means the necessity of rigorous observation in the course of military activities in information space of generally accepted norms and principles of international rights, such as respect for state sovereignty, non-interference in the internal affairs of other states, abstention from the use or threat of force, and the right of individual and collective self-defense."*[10]

Sovereignty is key to Russia's position. The country wants power over its space, including its information space. Russia is concerned about three gray areas in cyber war: preparation of the battlefield with information weapons, such as the alleged Chinese logic bombs in the U.S. power grid; cyber espionage; and propaganda.

Russia is especially concerned with the proliferation of logic bombs, one of the most dangerous forms of cyber attack, since hackers attempt to penetrate the sites of the Russian president, Duma and Federation Council a combined 10,000 times every day.[11] This could explain, in part, why Russia has called for a ban on logic bombs, as well as "trapdoors," which are access points built into software that allow easy access to attack at a later date. This makes sense in a strictly military context but banning information weapons is unenforceable because they are not subject to inspection. It is much more difficult to hide a 32-meter-long SS-18 Satan missile from inspectors than a 5-centimeter thumb drive. Such a ban would also be convenient for countries planning to continue stealing technology rather than developing it themselves.

Espionage is not sabotage, but at some point even cyber espionage could become cyber war. Espionage has long been considered acceptable under international law. Russia is within its rights to prohibit cyber espionage, or any kind of espionage, within its own borders. But Gen. Vladislav Sherstyuk, director of the Institute of Problems of Information Security at Moscow State University and former deputy secretary of the Russian Security Council, has proposed a treaty making cyber espionage illegal internationally.[12] It is interesting that a world leader in espionage would seek to ban it. Some suspect this means the Russians are confident in their ability not to get caught.

The difference between espionage and sabotage seems clear at first glance, but the methods and effects of cyber espionage have shifted the paradigm. Most agree that a single spy entering a country and collecting intelligence does not constitute an armed attack. But consider the nonstop flow of cyber attacks the Pentagon and other U.S. government agencies must divert precious resources to stopping every day, which could be compared to millions of spies sent by a government that does not care if you stop some or even most of them. This massive espionage has even been described as "death by a thousand cuts."[13] If the 1 million attacks the Pentagon must defend its networks against daily[14] does not yet rise to that level, surely at some point it must. Countries and individuals who engage in this form of espionage should consider the ramifications, particularly when it appears even more magnified to the targeted country when combined with other cyber espionage being attempted by numerous actors.

Espionage may appear more threatening than propaganda to Western eyes, but Russia has made a national defense issue out of the latter, calling for the "defense of [the] public information-psychological sphere from negative content."[15] During a recent speech in Moscow, Deputy Prime Minister Dmitry Rogozin called social networks part of a cyber war against Russia. "These sites allowed for government opponents to identify each other and organize themselves," he said. "Through this, they increase the number of people who receive special content that is undermining the authority of the state and the values of the established state."[16]

Russia blames Western propaganda enabled by cyberspace for the color revolutions of the early 2000s that led to the fall of Russia-friendly governments in several former Soviet states. The editor of the Russian journal *Geopolitika,* Leonid Savin, wrote:

> *"As history has shown, the governments of foreign states are often behind these structures (social sites), as was the case with the Rose revolution in Georgia and the Orange revolution in Ukraine. The U.S. government and various funds financed organizations that initiated disorder and acts of protest, prepared activists, secured media support, and even brought political pressure on the governments of countries, demanding they initiate 'democratic reforms.' "*[17]

Judging by the effects, we must acknowledge propaganda to be a form of warfare. It is simply a form of warfare that the U.S. has decided to allow because it considers restricting freedom of speech a greater evil and because it is confident of winning in the marketplace of ideas. This constitutes an irresolvable difference between the Western and Eastern conceptions of the value of freedom of speech. Keeping the Russian interpretation of propaganda as a form of war in mind, however, should help us see why the U.S. quest to nurture Western-style democracy since the end of the Cold War has elicited a more hostile response from post-Soviet Russia than we might otherwise have expected.[18]


AFP/GETTY IMAGES

Supporters of the Pirate Party rally in St. Petersburg against Internet censorship. The Russian government, which views online freedom differently from the West, believes that it has sovereignty over cyber networks within its borders.

Russians have gone beyond propaganda

in waging cyber war but it is unclear who bears responsibility. After the DDoS attacks against Estonia in 2007, a leader in Russia's state-funded Nashi youth movement and assistant in the Russian Duma, Konstantin Goloskokov, took credit but insisted he acted alone.[19] By contrast, the attacks against Georgia in 2008 appeared more coordinated.

The Russian-Georgian War, which included cyber attacks from both sides, began when Georgia attacked Russian troops who had occupied the breakaway Georgian territory of South Ossetia as peacekeepers. *Inside Cyber Warfare* author Jeffrey Carr writes that Georgia used cyber war first, attacking Ossetian websites, and Russia responded.[20] If Carr's version of events is correct, why does Russia continue to deny that it conducted cyber attacks against Georgia? From a legal standpoint, it seems the Russian government should have few concerns since these cyber operations occurred in the context of a shooting war and had little negative impact on civilians.

In all likelihood, Russia continues to deny responsibility for three reasons. The first reason is to protect itself from legal scrutiny, deserved or otherwise. The attackers defaced some commercial sites with no conceivable military objective.[21] A second reason could be to hide Russian capabilities and tactics. The cyber attacks against Georgia, in addition to relatively unsophisticated DDoS attacks, included more advanced attacks such as injections of the programming language SQL[22] and cross-site scripting (XSS).[23] If Russia had assumed responsibility for either attack, it would be acknowledging a military capability[24] and a willingness to use it.

A third, and likely primary, reason is to retain plausible deniability in the future. Russia relies on strategic ambiguity in the area of cyber. The physical evidence in the cyber attacks on Georgia is so unclear that most writers on the topic are quick to hedge, asserting, like Naval War College professor Michael Schmitt, that "there was no conclusive evidence that the Russian government conducted the attacks or was otherwise involved therein."[25] The government of Russia does not conduct cyber attacks itself.[26] Instead, it has trained, supported and funded a number of hacktivist groups, like the now-defunct Nashi, that know what they are expected to do and that they will not be punished for it.

Russia's emphasis on state sovereignty protects this capability. Carr writes: "The Kremlin will negotiate on military capabilities that they haven't used, but will not negotiate on their civilian hacker assets that they have used. In fact, the latter is considered an internal criminal matter not open to international negotiation at all."[27] So when a state claims to be the victim of a cyber attack originating in Russia, Russia can say that it has never conducted a cyber attack of its own, so it cannot be blamed. Absent physical proof of the attack originating from within the Kremlin, it is difficult to hold the government legally responsible for everything done in Russia with a computer. As Katharina Ziolkowski of the German Ministry of Defense observes, "taking into account the supposed indirect and quiet use of 'proxies,' e.g. patriotic hackers (hacktivists), by certain States, invoking State responsibility for cyber activities will very seldom meet the legal requirements as currently set by international jurisdiction and scholarly writings, i.e. the test of an 'effective' or 'overall' control of the State over the activities of the non-State actors."[28]

In her paper "Ten Rules for Cyber Security"[29] Enekin Tikk, project coordinator for the *Tallinn Manual*, addresses the issue of state responsibility for aggression originating from its territory by hashing out the "Responsibility Rule," proposed earlier by Schmitt,[30] and by adding a related "Cooperation Rule."

- RESPONSIBILITY RULE — The fact that a cyber attack has been launched from an information system located in a state's territory is evidence that the act is attributable to that state.[31]
- COOPERATION RULE — The fact that a cyber attack has been conducted via information systems located in a state's territory creates a duty to cooperate with the victim state.[32]

In other words, if a computer within state A launches a cyber attack against state B, state A bears a presumption of guilt, the responsibility rule, and must demonstrate its innocence by assisting state B in finding the real culprit. The official U.S. position is more ambiguous.

Georgians visit a military cemetery in Tbilisi in August 2013 during a ceremony in memory of the 2008 war with Russia. The war marked the use of cyber attack as part of a wider military strategy.

AFP/GETTY IMAGES

THE *TALLINN MANUAL*

The *Tallinn Manual on the International Law Applicable to Cyber Warfare,* written at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence by an independent international group of experts, is the result of a three-year effort to examine how extant international law norms apply to this "new" form of warfare. The *Tallinn Manual* pays particular attention to the *jus ad bellum,* the international law governing the resort to force by states as an instrument of their national policy, and the *jus in bello,* the international law regulating the conduct of armed conflict (also labeled the law of war, the law of armed conflict or international humanitarian law). Related bodies of international law, such as the law of state responsibility and the law of the sea, are dealt within the context of these topics.

Source: NATO CCDCOE

U.S. Department of State Legal Advisor Harold Koh has said that states will be held responsible for cyber attacks when they are conducted by individuals under that state's instructions, directions, or control.

"If a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it. These rules are designed to ensure that States cannot hide behind putatively private actors to engage in conduct that is internationally wrongful."[33]

"Control" could be interpreted broadly enough in the case of an authoritarian state or one with renowned policing capability.

Russia is especially concerned with the ambiguity, probably for fear that the U.S. will respond kinetically to cyber attacks originating in Russia. Savin writes: "Although governments declare that any cyber attack is deserving of a reactive response, it is necessary to draw the boundary where legal pursuit begins. The insistence that some attack is purposeful might be wrong."[34]

While hesitant to accept the responsibility rule, Russia has created the framework for the cooperation rule by signing an agreement[35] to create a communications link with the U.S. so that each party can inform the other of cyber activities in their information space that could be construed by the other as an attack. This could serve as a model to help prevent the further weaponization of cyberspace.

Conclusion and Recommendations

Russia is realizing that reliance on organized crime for the bulk of its cyber offensive capability is untenable in the long run. Internet service providers and other private entities are beginning to do the police work that Russia would not or could not do.[36]

We should also note that Russians are increasingly becoming victims as well. Not content with stealing from foreign interests, some cyber criminals are targeting Russians and thus directly challenging the state's authority and inadvertently providing common ground with the U.S. and Europe in the area of state sovereignty.[37] The U.S., Russia and the *Tallinn Manual* all concur: "States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."[38] International law could be written in such a way as to address mutual concerns about the Internet's vulnerability and encourage solutions for reducing it, including separating lawful military targets as much as possible from civilian infrastructure.

Russia must also be reassured that "responsibility" does not mean that if someone in Russia launches a cyber attack against a NATO country, it will automatically be considered an armed Russian attack, or that "cooperation" gives the attacked country an automatic right to examine the entirety of Russian cyberspace. The responsibility and cooperation rules can be interpreted broadly so as to let the international community decide case by case whether a country is doing its best to prevent international cyber attacks from within its borders and allow neutral parties to do the inspecting. Adopting some form of these rules, either unilaterally or with NATO, could force Russia's hand against organized crime and give hard-pressed Russian politicians a measure of political cover, while reducing the possibility of an

international misunderstanding that could lead to the outbreak of kinetic war.

At the same time, the international community should encourage Russia not to mistake responsibility for absolute control. As Swedish Foreign Affairs Minister Carl Bildt remarked at the 2013 Stockholm Internet Forum, Russian law now allows the state to "block websites without judicial oversight or transparency."[39] Even if Russia's motives are benign, the potential for abuse and violation of human rights is grave.

Finally, to reduce the potential for miscalculation, the bar should be lowered for self-defense against cyber attacks, provided the attacker's identity is certain. With most states now capable of conducting a cyber attack, a high standard for the use of force to respond to a cyber attack merely encourages aggressor states and nonstate actors to push the envelope. Of course, it is vital to positively identify the attacker, as difficult as that often is, before retaliating. With potential victims authorized to use force against cyber attacks that fall short of what legally constitutes an "armed attack," potential attackers will think twice, uncertain of whether they will face repercussions for their actions. □

1. A logic bomb is a piece of code emplaced into a victim's computer via the Internet. When emplaced into certain networks, such as the U.S. electric grid, it can inflict damage equal to or greater than a conventional explosive.
2. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010), 198.
3. Ibid., 63.
4. Chinese thought goes even further, viewing war as a constant and the military as but a single aspect of it. Sun Tzu, for example, viewed the state as in constant conflict, competition or tension with other powers. Occasionally the conflict involves military means, but it is always there.
5. An "armed attack" is the use of military force against a state on a scale that justifies that state to resort to self-defense. It may be contrasted with the "use of force," which is a smaller-scale hostile act, such as an embargo, that does not trigger a state's self-defense rights, and nonmilitary hostile acts, which are matters of criminal or civil law, not war.
6. Л.В. Савин, *Сетецентричная и Сетевая Война: Введение в Концепцию* (Москва: Евразийское Движение, 2011), 102.
7. С.И. Базылев, др., "Деятельность Вооруженных Сил Российской Федерации в Информационном Пространстве: Принципы, Правила, Меры Доверия." *Военная Мысль* 6 (июнь 2012): 25. http://www.ebiblioteka.ru/browse/doc/27601462 (accessed May 20, 2013).
8. Russian Federation, "Proposals for the Work of the Conference, Revision 1 to Document 27-E," WCIT Leaks, November 17, 2012. http://files.wcitleaks.org/public/S12-WCIT12-C-0027!R1!MSW-E.pdf (accessed June 19, 2013).
9. The U.S. military also considers cyber as a "domain," along with land, sea, air and space. David Perera, "Lynn: Cyberspace same as land, sea, air and space," FierceGovernmentIT, May 25, 2010. http://www.fiercegovernmentit.com/story/lynn-cyberspace-same-land-sea-air-and-space/2010-05-25#ixzz2s5YT9DjY (accessed February 1, 2014).
10. Базылев, "Деятельность Вооруженных Сил Российской Федерации в Информационном Пространстве," 27.
11. Иван Егоров, "Отобьем Кибератаки," Российская Газета 161 (июль 17, 2012): 2. http://www.ebiblioteka.ru/browse/doc/27406360 (accessed June 20, 2013).
12. Clarke, *Cyber War,* 229.
13 Sean Watts, "Low-Intensity Computer Network Attack and Self-Defense" in Raul A. Pedrozo and Daria P. Wollschlaeger, eds., *International Law and the Changing Character of War.* (Newport, RI: Naval War College, 2011), 72.
14. В. Гаврилов, "Взгляды Министерства Обороны США на Обеспечение Национальной Безопасности в Кибернетическом Пространстве," *Зарубежное Военное Обозрение* 7 (июль 2012): 3. http://www.ebiblioteka.ru/browse/doc/27608955 (accessed May 20, 2013).
15. I. N. Dylevsky, et al., "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect," *Military Thought* 1, vol. 16 (2007): 5. http://www.ebiblioteka.ru/browse/doc/24406039 (accessed May 22, 2013).
16. "Social networks part of cyber-war against Russia – Rogozin," Russia Today, June 7, 2013. http://rt.com/politics/part-cyber-war-rogozin-russia-354/ (accessed June 10, 2013).
17. Савин, *Сетецентричная и Сетевая Война,* 112.
18. Dylevsky, "Russian Federation Military Policy in the Area of International Information Security: Regional Aspect," 3.
19. Carr, Jeffrey, *Inside Cyber Warfare,* O'Reilly Media Inc., 2011, pg. 118.
20. Ibid., 18.
21. One of the *Tallinn Manual* authors, Professor Thomas Wingfield, notes that, even with no conceivable military objective in some of these attacks, they would not rise to the level of the "use of force" because there was no "real" damage done. Conversation with Wingfield.
22. SQL injections involve inserting code into databases to steal information from them, manipulate them or even assume administrator access over them.
23. XSS involves inserting malicious code into JavaScript routines, usually found in third-party advertising on websites, which is then activated whenever an unsuspecting user clicks on the link.
24. Such an admission would not guarantee that this represents the limits of Russia's cyber attack capability. They did not need to use their entire arsenal against small countries like Estonia and Georgia.
25. Schmitt, Michael N., "Cyber Operations and the Jus in Bello: Key Issues" (March 2, 2011), U.S. Naval War College *International Law Studies,* 2011, pg. 90.
26. If Russia's cyber war capability is anything like its cyber espionage capability, it has far more in its arsenal than is commonly known. The successor agencies to FAPSI (Federal Agency of Government Communication and Information), the Russian equivalent of the U.S. NSA, run a school in Voronezh that sanctions hackers. Clarke, Cyber War, 63.
27. Carr, *Inside Cyber Warfare,* 170.
28. Katharina Ziolkowski, "Ius ad Bellum in Cyberspace – Some Thoughts on the 'Schmitt-Criteria' for Use of Force" in Czosseck, C., R., Ottis, and K. Ziolkowski, eds. 2012 4th International Conference on Cyber Conflict (Tallinn, Estonia: NATO CCD COE Publications, 2012), 306.
29. Eneken Tikk, "Ten Rules for Cyber Security," *Survival: Global Politics and Strategy* 53, iss. 3 (2011): 129. http://dx.doi.org/10.1080/00396338.2011.571016 (accessed May 28, 2013).
30. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37, (1998-99): 913.
31. Tikk, "Ten Rules," 122.
32. Ibid., 123.
33. Harold H. Koh, "Koh's Remarks on International Law in Cyberspace, September 2012," Council on Foreign Relations, September 8, 2012. http://www.cfr.org/cybersecurity/kohs-remarks-international-law-cyberspace-september-2012/p29098 (accessed June 19, 2013).
34. Савин, *Сетецентричная и Сетевая Война,* 101.
35. Ellen Nakashima, "U.S. and Russia Sign Pact to Create Communication Link on Cyber Security," *The Washington Post,* June 17, 2013.
36. John Leyden, "Russian Cops Lack Kit to Fight Cybercrooks, Says Brit Security Buff," Register (London), June 6, 2013. http://www.theregister.co.uk/2013/06/06/private_sector_leading_russian_cybercrime_cleanup/ (accessed June 10, 2013).
37. This was the heart of the Russian Communications Ministry's proposal at Dubai. The problem was that it authorized strict control of content and not merely infrastructure.
38. Schmitt, Michael, N., "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed," *Harvard International Law Journal,* 2012, pg. 31.
39. Carl Bildt, speech at Stockholm Internet Forum 2013, May 22, 2013.