2011-09

Cyberwarfare

Berson, Thomas A.; Denning, Dorothy E.

IEEE

Berson, Thomas A., and Dorothy E. Denning. "Cyberwarfare." IEEE Security & Privacy 9.5 (2011): 13-15.
http://hdl.handle.net/10945/59867

Cyberwarfare

Thomas A. Berson
Anagram Laboratories

Dorothy E. Denning
Naval Postgraduate School

Cyberspace can serve as a source, tool, and target of conflict. As a source of conflict, it has given rise to new disputes in such areas as copyrights and intellectual property, free speech and censorship, privacy and surveillance, and Internet governance and telecommunications policy. As a tool of conflict, it facilitates all types of clashes, from street protests that are coordinated and promoted via websites and social media to state-on-state wars that rely on cyberspace to transmit information to the warfighter and coordinate military operations. As a target of conflict, its elements are subject to cyberattacks in support of state and nonstate battles. The articles in this special issue address this third area, with an emphasis on cyberattacks as an instrument of warfare, or what we refer to as *cyberwarfare*.

A New Battlefield

Cyberattacks have been a part of conflict for more than two decades. Early examples include

- the WANK worm, which infiltrated NASA's network in 1989 in protest of nuclear weapons and NASA's use of radioactive plutonium to fuel the Galileo probe's booster system;
- Strano Network's one-hour "netstrike" against French government websites in 1995 to protest French government policies on nuclear and social issues;
- the Electronic Disturbance Theatre's "Web sit-ins" against websites in Mexico, the US, and elsewhere starting in 1998 to support the Mexican Zapatistas, and later other political and social causes;
- the Internet Black Tigers' "suicide email bombings" against Sri Lankan embassies to counter government electronic propaganda; and
- Web defacements by Team Spl0it and other antiwar hackers calling for an end to the Kosovo conflict in 1999.

None of these were perpetrated by governments or tied to state-level conflicts. Rather, they were perpetrated by nonstate groups clashing with their own and international governments.

By the late 1990s, state-on-state conflict triggered many cyberattacks, though the acts themselves were conducted by nonstate actors. Patriotic hackers aimed their cyberattacks against foreign countries to support their own. Some of the cyberattacks during the Kosovo era were of that nature. For example, Serbian Black Hand hackers attacked the military computers of NATO countries, and Chinese hackers defaced US websites after their embassy in Belgrade was accidently destroyed by US airstrikes. The conflict was characterized as the first war on the Internet, in recognition of not only the cyberattacks but also the broader role played by the Internet, especially in the dissemination of information about the conflict.

Chinese hackers have been especially inclined toward patriotic hacking. Known as the Red Hacker Alliance or the Honker Union of China, they published a manifesto that expressed their patriotic mission and included Mao Zedong quotes. Their cyberattacks targets have included

- Indonesia in 1998 over the treat-

 1540-7993/11/$26.00 © 2011 IEEE COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES

ment of Chinese living in Jakarta;
- the US in 1999 after the Belgrade embassy bombing, and in 2001 following the death of a Chinese F-8 fighter pilot whose jet collided with a US EP-3 reconnaissance plane;
- Taiwan in 1999 following Taiwanese President Li Deng-Hui's advocacy for a "two-state theory," and in 2000 in conjunction with Taiwanese elections;
- Japan in 2000 over its handling of the Nanjing Massacre during WWII, and in 2004 over the disputed Diaoyu Islands; and
- Iran in 2010 in retaliation for the Iranian Cyber Army hijacking China's search engine, Baidu.

Many of these became two-way "hacker wars" between the Chinese hackers and their counterparts in other countries.

Russia has also been home to a contingent of patriot hackers. This was especially evident in 2007, when Estonia was hit by massive denial-of-service attacks over the controversial relocation of a Soviet-era war memorial, and in 2008, when Georgia was the target of similar attacks in conjunction with a ground confrontation with Russian troops. Russian hackers were also implicated for Web defacements during the 1999 Kosovo conflict and for various cyberattacks against Israel, the Ukraine, Lithuania, Chechnya, Belarus, Kyrgyzstan, and others during the past decade.

In This Issue

The Russian government has disavowed playing a role in any of these attacks. But even if it didn't plan or execute them, it might have encouraged or facilitated them, or at least turned a blind eye. The possibility of any government using its patriotic hackers as a kind of cybermilitia raises numerous issues related to the conduct of states and cyberwarfare.

This brings us to the first article of this special issue, "Cybermilitias and Political Hackers: Use of Irregular Forces in Cyberwarfare" by Scott D. Applegate, a US Army major. The article examines the implications of cybermilitias, whether explicitly controlled by their states or operating more or less independently. It addresses such issues as how these groups should be treated under international law, whether their activities violate the Law of Armed Conflict, patriotic hackers' combatant status, the extent to which states can control cybermilitias, and the problem of attributing cyberattacks. Applegate makes the important observation that, because of these issues, states might prefer to covertly leverage cybermilitias rather than openly conduct cyberwarfare with conventional forces.

Although nonstate actors appear to be responsible for most of the conflict-related cyberattacks that have been reported publicly, a few incidents are generally regarded as the work of states:

- After the KGB tried to infiltrate a Canadian company and steal software for controlling the Soviet's Trans-Siberian gas pipeline, the US planted a logic bomb in the code; the malware is thought to be responsible for the 1982 pipeline explosion.
- Israel purportedly used a cyberattack to disable Syrian air defenses prior to launching an airstrike against Syrian nuclear facilities in 2007.
- In 2010, the Stuxnet worm reportedly damaged centrifuges at Iran's nuclear enrichment facility at Natanz. Although we don't know the attack source, the level of sophistication suggests a nation-state. Israel, the US, China, and Russia have all been named as possibilities.

The second article, "Cyberwar Thresholds and Effects" by James A. Lewis, senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies, addresses difficult questions relating to nation-states' use of cyberspace as an instrument of armed conflict. Lewis examines the advantages and disadvantages of using cyberweapons, conditions under which cyberattacks are likely to be of value, scenarios for cyberwar, applicability of the international Laws of War and Armed Conflict, and thresholds for when a cyberevent becomes an act of war and use of force. More than 100 countries are reportedly developing capabilities for cyberespionage and cyberattack, so Lewis's article offers a timely analysis of just how and when those capabilities might be used to advantage.

The third article, "Principles of Cyberwarfare" by Raymond C. Parks and David P. Duggan of Sandia National Laboratories, offers principles for successfully conducting cyberwarfare. After examining whether long-held principles of warfare such as objective, mass, unity of command, and surprise extend to cyberwarfare, the authors present eight additional principles that are unique to the domain. The principles, which were derived from years of conducting red-team exercises equivalent to limited cyberwarfare scenarios, are offered as a starting point for discussion and dialogue.

The fourth and last article, "Deterring Strategic Cyberattack," is by David Elliott, an affiliate of Stanford University's Freeman Spogli Institute for International Studies and the Center for International Security and Cooperation. Rather than analyzing cyberwarfare's conduct or benefits, Elliott focuses on its deterrence, in particular, whether cyberattacks against essentially

civilian national infrastructure can be strategically deterred. He approaches the question by examining the elements of nuclear deterrence to ascertain their relevance to cyberdeterrence. After showing that the elements don't transfer, he offers deterrence by denial as the best solution.

These articles offer a fairly comprehensive introduction to the topic of cyberwarfare, particularly its policy and legal aspects. For readers interested in digging deeper and being exposed to other views, we offer the following suggestions.

The National Research Council has two excellent reports relating to cyberwarfare. The first—*Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*—is a report from the NRC Committee on Offensive Information Warfare.[1] It addresses issues relating to the US employing cyberwarfare, particularly cyberattack. The second—*Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*—is a collection of papers commissioned by the NRC and presented at a public workshop.[2] The papers offer a different perspective on topics discussed in this special issue, including cyberattacks' nature and conduct, cyberwarfare in international law, and cyberdeterrence.

The book *Cyber War* by Richard A. Clarke and Robert K. Knake offers an engaging and provocative look at cyberwarfare.[3] It includes a discussion of cyberincidents attributed to states, proposals for better defending against cyberattack threats, cyberwarfare strategies, and cyberpeace prospects.

Readers interested in original thinking on cyberwarfare are referred to the prescient paper by John Arquilla and David Ronfeldt called "Cyberwar Is Coming!"[4] In addition to introducing the term and concept of "cyberwar," the authors introduced "netwar," which involves information-related struggles associated with nonstate actors organized as networks.

Finally, cyberconflict at the nonstate level is discussed in greater depth in Dorothy Denning's paper, "Cyber Conflict as an Emergent Social Phenomenon."[5] The paper discusses hacktivism, electronic jihad, and patriotic hacking, and covers most of the examples mentioned earlier in this introduction along with many others. □

References

1. W.A. Owens et al., *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, Nat'l Academies Press, 2009.
2. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, Nat'l Academies Press, 2010.
3. R.A. Clarke and R.K. Knake, *Cyber War*, Basic Books, 2010.
4. J. Arquilla and D. Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy*, vol. 12, no. 2, 1993, pp. 141–165.
5. D.E. Denning, "Cyber Conflict as an Emergent Social Phenomenon," to be published in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, T. Hold and B. Schell, eds., IGI Global, 2011.

Thomas A. Berson *is the founder of Anagram Laboratories. Contact him at berson@anagram.com.*

Dorothy E. Denning *is Distinguished Professor of Defense Analysis at the Naval Postgraduate School. Contact her at dedennin@nps.edu.*