2012-08

When is a cyberattack a use of force or an armed attack?

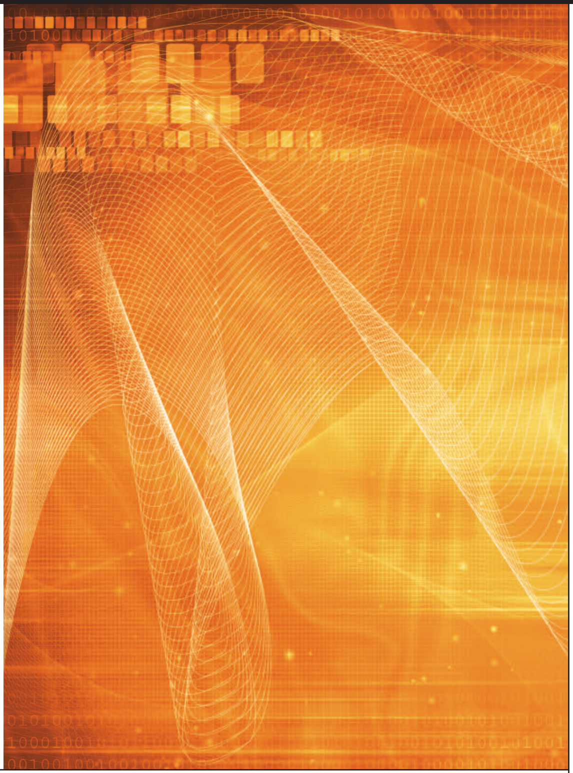
Boothby, William H.; von Heinegg, Wolff Heintschel; Michael, James Bret; Schmitt, Michael N.; Wingfield, Thomas C.

IEEE

W.H. Boothby, W.H. von Heinegg, J.B. Michael, M.N. Scmitt, T.C. Wingfield, "When is a cyberattack a use of force or an armed attack?", Computer, (August 2012), pp. 82-84.
http://hdl.handle.net/10945/56533

When Is a Cyberattack a Use of Force or an Armed Attack?

William H. Boothby
Royal Air Force (Retired), United Kingdom
Wolff Heintschel von Heinegg
Europa-Universität Viadrina, Germany
James Bret Michael
Naval Postgraduate School
Michael N. Schmitt
US Naval War College
Thomas C. Wingfield
George C. Marshall European Center for Security Studies



A cyberattack involving military or intelligence operations might not rise to the level of a "use of force" under international law.

News reports and public discussion about cyberattacks appear daily in traditional and social media. Cyberattacks used in the commission of crimes, such as stealing customer credit card information, defacing websites, distributing child pornography via file-sharing sites, and creating and leasing out botnets, have become commonplace. Moreover, cyberattacks that once were considered extraordinary—in particular, those carried out as part of state-sponsored military or intelligence operations—will likely increase in frequency and severity.

RECENT CYBERATTACKS

Several such cyberattacks have occurred recently. For instance, the US, together with Israel, allegedly used two sophisticated viruses, Flame and Stuxnet, to disrupt Iran's petroleum production and distribution infrastructure and its uranium-enrichment facilities (E. Nakashima, G. Miller, and J. Tate, "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say," *The Washington Post*, 19 June 2012).

Another cyberattack targeted human rights activists acting on behalf of ethnic Uyghurs in the Xinjiang Uyghur Autonomous Region and other parts of China (B. Prince, "Mac, Windows Malware Campaign Targets Uyghur Activists," *eWeek*, 29 June 2012; www.eweek.com/c/a/Security/Mac-Windows-Malware-Campaign-Targets-Uyghur-Activists-370913). The attackers—allegedly working for the People's Republic of China—used relatively unsophisticated malware, in the form of a Trojan horse that installs a rootkit, to track the Uyghur activists' activities and exfiltrate data from their computers.

Even the Arab uprisings have seen cyberattacks. Recently, a group of progovernment Syrian hacktivists, who call themselves the Syrian Electronic Army, conducted cyberattacks against Al-Arabiya News, Al-Jazeera, and other news organizations that it accused of spreading misinformation about the widening conflict in Syria (P.J. Watson, "Syrian Hacktivists Launch Al-Jazeera Cyber Attack," *Infowars*, 5 July 2012; www.infowars.com/syrian-activists-launch-al-jazeera-hack-attack).

Although cyberattacks involving military or intelligence operations could violate domestic or international law, they don't always rise to the level of a use of force or armed attack under the international law that governs the legality of the use of force, also known as *jus ad bellum*.

Judging by the dialogue so far, people who aren't well versed in international law frequently mischaracterize the legal nature of cyberattacks. This is unfortunate because the legality of cyberattacks under *jus ad bellum*, as well as any

Published by the IEEE Computer Society

0018-9162/12/$31.00 © 2012 IEEE

response to such actions, depends on whether these attacks reach particular legal thresholds.

ARMED ATTACKS IN CYBERSPACE

International customary law (legal norms that have developed through state practice), now codified in UN Charter Article 2(4), provides that states are prohibited from engaging in the use of force. When they do so, they violate international law unless they are granted authorization from the UN Security Council to conduct the operation or are responding to an armed attack. The latter justification, set forth in UN Charter Article 51, reflects customary international law. This raises the question of when a cyberattack amounts to an armed attack that permits the victim state to respond with the use of force.

The applicable *lex lata* (the law currently governing conflict) predates the modern computing era. It was intended to address concerns about kinetic and other noncyber forms of warfare. Nevertheless, legal experts agree that international law applies to cyberoperations because they can potentially have effects equivalent to those realized via noncyber (kinetic) means.

Although no precise definition exists for the term "use of force" under international law, most experts agree that it includes cyberattacks that cause physical damage or injure individuals. An "armed attack" is a use of force carried out by an organ of a state, an entity working on a state's behalf, or an organized nonstate group that results in "grave" scale and effects.

Although there is no bright-line scale-and-effects test to distinguish grave from nongrave consequences, legal experts generally agree that to qualify as an armed attack, a cyberattack must result in death or a significant degree of injury to persons or physical damage to property. Once it does, the victim state can respond with kinetic or nonkinetic means, as long as the response is necessary under the circumstances and uses no more force than required to defend the state.

ARMED ATTACKS VERSUS CYBERATTACKS

Did the Flame virus constitute a use of force or an armed attack triggering the right of self-defense? According to *The Washington Post*, "the massive piece of malware secretly mapped and monitored Iranian computer networks, sending back a steady stream of intelligence to prepare for a cyberwarfare campaign." Given only this information about the cyberoperation, this was neither a use of force by any state that might have launched it, nor an armed attack that would permit the victim state to respond with its own use of force. Although the attackers used Flame to gather intelligence about a military target (petroleum-export facilities), they didn't physically damage those facilities or otherwise render them inoperable.

Legal experts generally agree that to qualify as an armed attack, a cyberattack must result in death or a significant degree of injury to persons or physical damage to property.

The use of Stuxnet against Iran's uranium-enrichment facilities is more difficult to categorize. Because the facilities suffered physical damage, the attack qualifies as a use of force and, unless the attacking state was acting in self-defense, the operation violates international law. Iran can respond legally with a use of force only if the operation targeting it qualifies as an armed attack owing to its gravity. Because the precise scale and effects necessary to qualify the operation as an armed attack are uncertain in international law, this matter remains unresolved.

The use of the Backdoor OSX MaControl.b malware against Uyghur activists was not in violation of the use of force prohibition because it fell below the use of force threshold: it was a limited-scale intelligence-gathering operation that caused no physical damage to the targeted computing devices. Moreover, under international law, it is questionable whether the use of force prohibition applies when a state uses force against a nonstate actor (although the state might violate other aspects of international law).

Because the Syrian Electronic Army is not a state, the use of force prohibition does not apply—although, again, the cyberattacks might violate other aspects of international and domestic law. Even if the prohibition had applied, the Syrian Electronic Army's cyberattack on Al-Jazeera's @AJStream Twitter account did not measurably damage computing systems and thus would not qualify as a use of force: it only served as a means for the group to send tweets containing its version of events transpiring in Syria.

Similarly, the group's defacement of the Al-Arabiya News website would not qualify. In this case, the relevant legal question was whether these actions amounted to an armed attack that would justify a forceful response by states in which the media organizations were located. In light of the absence of physical damage, they clearly didn't.

Not all cyberattacks are uses of force or armed attacks. In fact, no cyberattack to date has been proven to be an armed attack. However, it's technically feasible to carry out armed attacks in cyberspace, and some states have publicly acknowledged that cyberoperations are an indispensible part of modern warfare.

To fully understand these aspects of the *jus ad bellum*, readers should look for the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, to be published in early 2013 by Cambridge University Press. This book summarizes, in the form of black-letter rules and extensive commentary, the consensus among today's top legal experts on how international law applies to cyberwarfare. It should prove useful to policymakers and legal advisers involved in determining proposed cyberoperations' legality.

William H. Boothby *is an Air Commodore (retired) and served as the deputy director of legal services for the Royal Air Force, United Kingdom. Contact him at williamboothby@hotmail.com.*

Wolff Heintschel von Heinegg *is a professor of international law at Europa-Universität Viadrina, Frankfurt, Germany. Contact him at heintschelvonheinegg@europa-uni.de.*

James Bret Michael *is a professor in the Computer Science and Electrical and Computer Engineering departments at the Naval Postgraduate School. Contact him at bmichael@nps.edu.*

Michael N. Schmitt *is a professor and chairman of the International Law Department at the US Naval War College. Contact him at schmitt@aya.yale.edu.*

Thomas C. Wingfield *is a professor of international law at the George C. Marshall European Center for Security Studies. Contact him at thomas.c.wingfield@marshallcenter.org.*

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements of the North Atlantic Treaty Organization or the governments of Germany, the UK, or the US.

Editor: Jeffrey Voas, National Institute of Standards and Technology; jeffrey.m.voas@gmail.com

stay connected.
Keep up with the latest IEEE Computer Society publications and activities wherever you are.