Was Stuxnet an Act of War? Decoding a Cyberattack

David P. Fidler
Indiana University

Violations of privacy online threaten an individual's sense of security—and relate to the problem of protecting human security in cyberspace. In the cyber and noncyber realms, prospects for human security are shaped by policies designed to achieve other security objectives, especially national security. Thus, how governments manage the potential for cyberconflict and cyberwar affects whether human security and an individual's privacy can be protected. We face a cyber version of the age-old problem that human rights suffer where war exists or preparations for conflict advance, which raises the need to address an event not immediately associated with information privacy—Stuxnet.

The cybersecurity community considers the Stuxnet worm to be "game-changing" malware because of its sophistication, purpose, and implications. The development and release of Stuxnet brought the world closer to realizing predictions that cybertechnologies would more directly impact realpolitik. The technical decoding of Stuxnet triggered efforts to decipher what this seminal episode means for international politics.

As software, we now understand this worm. As a political event, we're still debating its significance. Although consensus doesn't exist, reactions to Stuxnet suggest that the worm's political repercussions may surpass its technical achievements—impact that might affect conditions influencing online privacy.

Cybershot Heard 'Round the World

Technical analysis of Stuxnet revealed a complex piece of malware with multiple unprecedented features that take cybersecurity into a new dimension. Among its many features, Stuxnet

- exploited four 0-day vulnerabilities in Microsoft Windows software;
- used two stolen digital certificates to mask its malicious code;
- targeted specific programmable logic controllers (PLCs) operating on industrial control systems attached to Iranian centrifuges engaged in enriching uranium;
- modified PLC software to cause the centrifuges to spin at speeds that would damage them;
- hid the altered speeds from verification systems through code that recorded and played back information indicating normal operating conditions;
- was disseminated in three variants before discovery;
- spread by various means, including removable drives, two Microsoft Windows 0-day vulnerabilities, and the Internet;
- reportedly caused damage to approximately 1,000 centrifuges; and
- incorporated features to minimize collateral damage and terminate the worm's activities on a set date.[1]

In short, Stuxnet was a technologically sophisticated, purpose-built, and precisely engineered cyberweapon used in the context of one of the world's most dangerous political issues—possible Iranian nuclear proliferation. Everything about Stuxnet was high stakes. For this reason, intense interest has arisen around who was responsible for Stuxnet. However, attribution raises questions about what, politically and legally, the perpetrators did. Was it an act of war? Cybersabotage? Mere espionage? Only a virtual violation of Iranian sovereignty?

The Other Code

Characterizing what Stuxnet's creators did requires understanding how a different code—international law—applies to this incident. Reviewing Stuxnet's features, many international lawyers would see a deliberate, offensive, and sustained act undertaken through unprecedented means or methods, intended to cause physical damage or destruction, and perpetrated in all likelihood by a state or states against a perceived national security threat from a rival power.

In simple terms, Stuxnet's re-

 1540-7993/11/$26.00 © 2011 IEEE

lease looks like an act of war. However, as with Stuxnet's code, nothing about international law is simple. Indeed, international law doesn't apply the concept of "act of war" in evaluating the legality of state violence. Rather, international lawyers assess whether actions constitute an illegal "intervention," "use of force," "armed attack," or "aggression." This assessment involves interpreting these concepts in international law (doctrinal analysis) and understanding how states react to events (evaluation of state practice).

As a matter of doctrine, international law prohibits a state from intervening in the domestic affairs of other states, using force against another state, or engaging in acts of aggression. A state can only legally use force if it's the victim of an armed attack or if the United Nations Security Council has authorized it.

These rules establish thresholds that distinguish an intervention from a use of force, and a use of force from an armed attack. Acts of aggression involve more serious uses of force and armed attacks. Determining into which category state behavior falls was difficult well before the emergence of cyberweapons. International law has experienced controversies concerning whether certain actions crossed the use-of-force or armed-attack threshold. As the International Court of Justice has ruled, not all uses of force constitute armed attacks.[2] Similarly, some damaging covert actions are illegal interventions but not uses of force. Determining which type of threshold an action crosses usually involves evaluating its effects or consequences on a case-by-case basis.

Doctrinally, this approach uses the following criteria to assess whether an incident constitutes an intervention, use of force, or armed attack:

- instrumentalities—the means or methods used,
- effects—the damage to tangible objects or injury to humans,
- gravity—the damage or injury's scale or extent,
- duration—the incident's length of time,
- intent—the purpose behind the act(s) in question, and
- context—the circumstances surrounding the incident.

Applying these criteria to Stuxnet, a plausible argument can be made that its deployment constituted an illegal use of force, armed attack, and act of aggression. The instrumentality used was a purpose-built cyberweapon—highly sophisticated and precisely targeted malware. The malware's design demonstrates that it was intended to cause physical damage—and the worm reportedly caused significant damage—to specific tangible objects in a particular location in one country: the uranium-enrichment centrifuges at Natanz, Iran.

This target corresponded with growing tensions over Iranian nuclear facilities and programs, as evidenced by multiple rounds of UN Security Council sanctions against Iran. In terms of duration, dissemination of the worm began in 2009, it was discovered in 2010, and the worm included a 2012 date on which it would erase itself—demonstrating that the Stuxnet attack wasn't a brief episode in intent, design, and execution. It was also of significant intensity, with the perpetrators releasing three variants of the worm before it was identified—evidence of ongoing monitoring and manipulation of the situation—and infecting "air-gapped" PLC systems through infected removable drives, revealing penetration of Iranian security systems at the Natanz facility.

Although important, doctrinal analysis alone is insufficient to determine how international law applies to events. International lawyers must also consider how states respond to incidents because state practice helps reveal how states view such incidents politically and legally. States shape the meaning and interpretation of international legal rules through their behavior, which is particularly important in areas in which international agreements don't define concepts such as use of force and armed attack. When we turn to state practice involving Stuxnet, what we find doesn't support the doctrinal analysis sketched above.

The Sound of Silence

Nation-states have been curiously quiet about Stuxnet. Although commentators have frequently used "war" and "attack" to describe this unprecedented event, states have refrained from applying international law on the use of force, armed attack, and aggression. This reaction cuts across all kinds of states, including the victim state (Iran), actual and emerging great powers not suspected of involvement (for example, China, Russia, and India), and developing countries that are vulnerable to new weaponized technologies. Typically, states make their political and legal positions publicly known concerning major incidents that raise use-of-force questions, a process that usually generates controversies created by diverse state practice.

For example, high-profile, non-cyber operations that cause significant physical damage in a country inflicted deliberately by another state with hostile intent tend to provoke controversy among states about how international law applies to these operations. However much these controversies muddy the waters concerning state practice in international legal analysis, lawyers usually expect a diversity of practice as states, politically and

legally, jockey for position. What are we to make of the silence surrounding Stuxnet—the most significant cyberincident to date?

We might be moving toward cyber-centric international legal rules, but not in the manner envisioned by those seeking negotiated constraints on cybertechnologies.

In international politics, states know that silence has importance for interpreting international law, especially during major developments. Determining what silence means for state practice is tricky, particularly in a context with few incidents to evaluate. Generally speaking, however, international lawyers perceive silence as acquiescence to the legal implications of actions or incidents. With Stuxnet, silence across the international system suggests that states don't perceive this situation triggered the rules on the use of force, armed attack, and aggression. The reasons states have been quiet about Stuxnet might differ, but the cumulative effect of consistent state practice has legal impact and implications for cybertechnology use.

What followed Stuxnet contributes to a trend in the cyberrealm toward convergence of state practice rather than controversy. As more state practice accumulates and as the scale and intensity of some cyberoperations, including espionage, increase, we're seeing less diversity in state practice. Before the most relevant cyberincidents—the distributed denial-of-service (DDoS) attacks on Estonia in 2007 and Georgia in 2008, followed by Stuxnet—states debated whether international legal action was necessary to address the threat cybertechnologies could pose to international peace and security. For instance, in the late 1990s, Russia proposed negotiations to establish rules for the conduct of information warfare.[3] Nothing resulted from these efforts because states disagreed about the threat and the remedy—but we had, however superficial, diverse views on the threat and its relationship to international law.

In the case of the DDoS attacks on Estonia, the Estonian government argued it was the victim of an armed attack, but its NATO allies and Russia opposed this characterization. We still have diversity in state practice, but the victim state is in the minority. The DDoS attacks on Georgia occurred in conjunction with a conventional military conflict with Russia, which subordinated the cyber-elements of this war in evaluating it under the laws of armed conflict.

Then comes Stuxnet—the kind of deliberate, hostile, highly sophisticated, state-created, and critical-infrastructure-threatening offensive use of malware that has worried cybersecurity experts since the 1990s, if not before. But we have silence from states—including the victim state—in terms of international law on the use of force about the first use of exactly the kind of cyberweapon people feared would emerge. Iran's failure to appeal to international law on the use of force, even if just to score political points against Stuxnet's "usual suspects" (Israel and the US), is particularly interesting for numerous reasons, including the victim state's typical condemnation of attack and Iran's propensity not to miss opportunities to make political hay at the expense of the US and Israel.

Stuxnet taps directly into concerns experts have long had about cyberweapons—namely, that such weapons could inflict significant physical damage like kinetic weapons as well as different types of damage kinetic weapons can't achieve. In other words, the nature of the weapon, as well as its potential for causing damage, has been at issue. But despite Stuxnet bringing long-standing fears about cyberweapons to life, there appears to be a strange conspiracy of silence among states about this unprecedented cyberepisode.

Now What?

Before Stuxnet, debates about international law and cybertechnologies frequently featured two positions:

- governments can readily apply existing rules without tailoring them to the cybercontext, and
- the potential of cybertechnologies fundamentally challenges existing rules, which requires developing new cyber-centric norms that limit the dangers these technologies pose.

However, after Stuxnet, a third route is emerging—the development of cyber-specific rules that increase the political and legal space in which states can use cybertechnologies against one another. In short, we might be moving toward cyber-centric international legal rules, but not in the manner envisioned by those seeking negotiated constraints on cybertechnologies.

This reading of state practice in the wake of Stuxnet suggests that states, particularly the big cyberpowers, are seeking to establish higher use-of-force and armed-attack thresholds for cyber-based actions to permit more room to explore and exploit cybertechnologies as instruments of foreign policy and national security. For example, states engage in cyberespionage on a scale, intensity, and intrusiveness that signals a tolerance for covert cyberopera-

tions that can impose greater adverse political, economic, and military consequences on governments than noncyber actions considered illegal threats or uses of force. Similarly, although Stuxnet caused serious damage to Iranian centrifuges through exploitation of cyber-controlled physical systems, states—including Iran—haven't denounced this incident as an illegal use of force or armed attack, even though such damage caused by conventional, kinetic means would have triggered such accusations. State practice arguably categorizes Stuxnet as a covert cyberaction that didn't cross the threshold into a use of force.

Supporting this line of reasoning are moves by the great powers—especially China, Russia, and the US—toward enhancing their capabilities for covert, defensive, and offensive cyberoperations and exploring ways to utilize these capabilities. Neither the international law inherited from the noncyber realm nor negotiated restrictions on cybertechnologies provide the most conducive environment for this trajectory. Instead, through and after Stuxnet, we see states in the process of generating cyber-specific rules that permit significant freedom of cyberaction.

Speculation about what Stuxnet means for cybersecurity will continue in both the technical and political realms. Technically, Stuxnet has raised the bar, setting a precedent that, as experts warn, others will seek to repeat and surpass. Politically, state behavior after Stuxnet appears calculated to create legal and policy space for cyberoperations that can push boundaries in the post-Stuxnet world. What is happening is eerily familiar from past experiences of emerging weapons technologies and deeply disconcerting given the "unknown unknowns" a world resigned to cyberconflict will confront. If the noncyber world is any guide, increased prospects for conflict between nations represent grim news for human security and human rights, including the right to privacy. ☐

References

1. N. Falliere, L.O. Murchu, and E. Chien, *W32. Stuxnet Dossier*, Symantec Security Response, version 1.4, Feb. 2011.
2. "Case Concerning the Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Merits)," *Int'l Court of Justice Reports*, 27 Jun. 1986, p. 14; www.icj-cij.org/docket/files/70/6503.pdf.
3. P.A. Johnson, "An Assessment of International Legal Issues in Information Operations," US Dept. of Defense, May 1999; http://handle.dtic.mil/100.2/ADB257057.

***David P. Fidler** is the James Louis Calamaras Professor of Law at the Indiana University Maurer School of Law and is a fellow at the Indiana University Center for Applied Cybersecurity Research. Contact him at dfidler@indiana.edu.*