ISN
ETH Zurich

23 October 2012

A Stuxnet Future? Yes, Offensive Cyber-Warfare is Already Here

According to Mihoko Matsubara, the Stuxnet attack on Iran's nuclear facilities demonstrates that well-resourced actors now have the capacity to use offensive cyber capabilities to fragment command and control structures, disrupt critical infrastructures, and undermine other components of national security in major ways.

By Mihoko Matsubara for ISN

Mounting Concerns and Confusion

Stuxnet proved that any actor with sufficient know-how in terms of cyber-warfare can physically inflict serious damage upon any infrastructure in the world, even without an internet connection. In the words of former CIA Director Michael Hayden: "The rest of the world is looking at this and saying, 'Clearly someone has legitimated this kind of activity as acceptable international conduct'."

Governments are now alert to the enormous uncertainty created by cyber-instruments and especially worried about cyber-sabotage against critical infrastructure. As US Secretary of Defense Leon Panetta warned in front of the Senate Armed Services Committee in June 2011; "the next Pearl Harbor we confront could very well be a cyber-attack that cripples our power systems, our grid, our security systems, our financial systems, our governmental systems." On the other hand, a lack of understanding about instances of cyber-warfare such as Stuxnet has led to confused expectations about what cyber-attacks can achieve. Some, however, remain excited about the possibilities of this new form of warfare. For example, retired US Air Force Colonel Phillip Meilinger expects that "[a]… bloodless yet potentially devastating new method of war" is coming. However, under current technological conditions, instruments of cyber-warfare are not sophisticated enough yet to deliver a decisive blow to the adversary. As a result, cyber-capabilities still need to be used alongside kinetic instruments of war.

Advantages of Cyber-Capabilities

Cyber-capabilities provide three principal advantages to those actors that possess them. First, they can deny or degrade electronic devices including telecommunications and global positioning systems in a stealthy manner irrespective of national borders. This means potentially crippling an adversary's intelligence, surveillance, and reconnaissance capabilities, delaying an adversary's ability to retaliate (or even identify the source of an attack), and causing serious dysfunction in an adversary's command and control and radar systems.

Second, precise and timely attribution is particularly challenging in cyberspace because skilled perpetrators can obfuscate their identity. This means that responsibility for attacks needs to be attributed forensically which not only complicates retaliatory measures but also compromises attempts to seek international condemnation of the attacks.

Finally, attackers can elude penalties because there is currently no international consensus as to what actually constitutes an ‘armed attack’ or ‘imminent threat’ (which can invoke a state’s right of self-defense under Article 51 of the UN Charter) involving cyber-weapons. Moreover, while some countries - including the United States and Japan - insist that the principles of international law apply to the 'cyber' domain, others such as China argue that cyber-attacks “do not threaten territorial integrity or sovereignty.”

Disadvantages of Cyber-Capabilities

On the other hand, high-level cyber-warfare has three major disadvantages for would-be attackers. First, the development of a sophisticated ‘Stuxnet-style’ cyber-weapon for use against well-protected targets is time- and resource- intensive. Only a limited number of states possess the resources required to produce such weapons. For instance, the deployment of Stuxnet required arduous reconnaissance and an elaborate testing phase in a mirrored environment. F-Secure Labs estimates that Stuxnet took more than ten man-years of work to develop, underscoring just how resource- and labor- intensive a sophisticated cyber-weapon is to produce.

Second, sophisticated and costly cyber-weapons are unlikely to be adapted for generic use. As Thomas Rid argues in "Think Again: Cyberwar,” different system configurations need to be targeted by different types of computer code. The success of a highly specialized cyber-weapon therefore requires the specific vulnerabilities of a target to remain in place. If, on the contrary, a targeted vulnerability is ‘patched’, the cyber-operation will be set back until new malware can be prepared. Moreover, once the existence of malware is revealed, it will tend to be quickly neutralized – and can even be reverse-engineered by the target to assist in future retaliation on their part.

Finally, it is difficult to develop precise, predictable, and controllable cyber-weapons for use in a constantly evolving network environment. The growth of global connectivity makes it difficult to assess the implications of malware infection and challenging to predict the consequences of a given cyber-attack. Stuxnet , for instance, was not supposed to leave Iran’s Natanz enrichment facility, yet the worm spread to the World Wide Web, infecting other computers and alerting the international community to its existence. According to the *Washington Post* , US forces contemplated launching cyber-attacks on Libya’s air defense system before NATO’s airstrikes. But this idea was quickly abandoned due to the possibility of unintended consequences for civilian infrastructure such as the power grid or hospitals.

Implications for Military Strategy

Despite such disadvantages, cyber-attacks are nevertheless part of contemporary military strategy including espionage and offensive operations. In August 2012, US Marine Corps Lieutenant General Richard Mills confirmed that operations in Afghanistan included cyber-attacks against the adversary. Recalling an incident in 2010, he said, "I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."

His comments confirm that the US military now employs a combination of cyber- and traditional offensive measures in wartime. As Thomas Mahnken points out in “Cyber War and Cyber Warfare,” cyber-attacks can produce disruptive and surprising effects. And while cyber-attacks are not a direct cause of death, their consequences may lead to injuries and loss of life. As Mahnken argues, it would be inconceivable to directly cause Hiroshima-type damage and casualties merely with cyber-attacks. While a “cyber Pearl Harbor” might shock the adversary on a similar scale as its namesake in 1941, the ability to inflict a decisive, extensive, and foreseeable blow requires kinetic support – at least under current technological conditions.

Implications for Critical Infrastructure

Nevertheless, the shortcomings of cyber-attacks will not discourage malicious actors in peacetime. The anonymous, borderless, and stealthy nature of the 'cyber' domain offers an extremely attractive asymmetrical platform for inflicting physical and psychological damage to critical infrastructure such as finance, energy, power and water supply, telecommunication, and transportation as well as to society at large. Since well before Stuxnet, successful cyber-attacks have been launched against vulnerable yet important infrastructure systems. For example, in 2000 a cyber-attack against an Australian sewage control system resulted in millions of liters of raw sewage leaking into a hotel, parks, and rivers.

Accordingly, the safeguarding of cyber-security is an increasingly important consideration for heads of state. In July 2012, for example, President Barack Obama published an op-ed in the *Wall Street Journal* warning about the unique risk cyber-attacks pose to national security. In particular, the US President emphasized that cyber-attacks have the potential to severely compromise the increasingly wired and networked lifestyle of the global community. Since the 1990s, the process control systems of critical infrastructures have been increasingly connected to the Internet. This has unquestionably improved efficiencies and lowered costs, but has also left these systems alarmingly vulnerable to penetration. In March 2012, McAfee and Pacific Northwest National Laboratory released a report which concluded that power grids are rendered vulnerable due to their common computing technologies, growing exposure to cyberspace, and increased automation and interconnectivity.

Despite such concerns, private companies may be tempted to prioritize short-term profits rather than allocate more funds to (or accept more regulation of) cyber-security, especially in light of prevailing economic conditions. After all, it takes time and resources to probe vulnerabilities and hire experts to protect them. Nevertheless, leadership in both the public and private sectors needs to recognize that such an attitude provides opportunities for perpetrators to take advantage of security weaknesses to the detriment of economic and national security. It is, therefore, essential for governments to educate and encourage --- and if necessary, fund --- the private sector to provide appropriate cyber-security in order to protect critical infrastructure.

Implications for Espionage

The sophistication of the Natanz incident, in which Stuxnet was able to exploit Iranian vulnerabilities, stunned the world. Advanced Persistent Threats (APTs) were employed to find weaknesses by stealing data which made it possible to sabotage Iran’s nuclear program. Yet APTs can also be used in many different ways, for example against small companies in order to exploit larger business partners that may be possession of valuable information or intellectual property. As a result, both the public and private sectors must brace themselves for daily cyber-attacks and espionage on their respective infrastructures. Failure to do so may result in the theft of intellectual property as well as trade and defense secrets that could undermine economic competitiveness and national security.

In an age of cyber espionage, the public and private sectors must also reconsider what types of information should be deemed as “secret,” how to protect that information, and how to share alerts with others without the sensitivity being compromised. While realization of the need for this kind of wholesale re-evaluation is growing, many actors remain hesitant. Indeed, such hesitancy is driven often out of fears that doing so may reveal their vulnerabilities, harm their reputations, and benefit their competitors. Of course, there are certain types of information that should remain unpublicized so as not to damage the business, economy, and national security. However, such classifications must not be abused against balance between public interest and security.

Cyber-Warfare Is Here to Stay

The Stuxnet incident is set to encourage the use of cyber-espionage and sabotage in warfare. However, not all countries can afford to acquire offensive cyber-capabilities as sophisticated as Stuxnet and a lack of predictability and controllability continues to make the deployment of cyber-weapons a risky business. As a result, many states and armed forces will continue to combine both kinetic and 'cyber' tactics for the foreseeable future. Growing interconnectivity also means that the number of potential targets is set to grow. This, in turn, means that national cyber-security strategies will need to confront the problem of prioritization. Both the public and private sectors will have to decide which information and physical targets need to be protected and work together to share information effectively.

Mihoko Matsubara is a cybersecurity analyst. She is also a non-resident research fellow at the Pacific Forum CSIS, Honolulu. Mihoko received her MA in International Relations and Economics from the Paul H. Nitze School of Advanced International Studies, Johns Hopkins University, on Fulbright.

Publisher

International Relations and Security Network (ISN)

http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=154091&lng=en