The New Nuke?

by Yusuf Sezer

Over the past few decades, the major nations of the world have readily adopted and integrated computer technologies into their social, economic, political, and military sectors. Trading on the stock market, conducting military operations, directing the world's flight traffic, and delivering electricity to millions of people are just a few examples of the many critical real-world processes that rely on computer systems. As events in the past few years have shown, these computer systems—and the real-world processes that depend on them—can be exploited with "'illegal or legally ambiguous digital tools' like website defacements, information theft, website parodies, DoS attacks, virtual sit-ins, and virtual sabotage" (Hampson 514). Thus, nations that have high levels of technological development—and thus high technological dependence—are vulnerable to cyber-attacks (Sanger). This fundamental weakness shared by major world powers has ushered in a new type of militaristic weapon that poses a threat to global peace.

The definition of a cyber weapon varies from source to source, but most agree that cyber weapons refer to the strategic use of malware—programs that are designed to damage or disrupt computer systems—for militaristic purposes. Perhaps the most notable example of a cyber weapon is Stuxnet, a piece of malware that was designed to infiltrate computer systems in Iran's Natanz uranium enrichment plant (Farwell and Rohozinski). Although no government has officially claimed responsibility for the development and deployment of Stuxnet, interviews with both former and current American, Israeli, and European officials strongly suggest that the attack was orchestrated by Israel and the United States (Sanger). Farwell and Rohozinski explain that Stuxnet's goal was to destroy the plant's centrifuges by causing them to spin much faster than normal, thus slowing Iran's nuclear program—an objective that aligns with American and Israeli political goals. Stuxnet succeeded in destroying many centrifuges and set a new precedent for the possibilities of cyber weaponry. Unlike the malware that came before it, "Stuxnet wasn't about industrial espionage: it didn't manipulate, or erase information. Rather, Stuxnet's goal was to physically destroy a military target… literally" (Farwell and Rohozinski).

Although Stuxnet was successful in slowing Iran's nuclear program, the scale of the damage it caused is relatively small when compared to the full-potential of cyber weapons. In *The Basics of Cyber Warfare*, Jason Andress and Steve Winterfield point out that cyber weapons could be employed as "Weapons of Mass Disruption." The idea is to use cyber weapons to disrupt computer systems that control major infrastructure (Andress and Winterfield 21). In a speech at the Cybersecurity and Consumer Protection Summit, President Obama recognized that:

> much of [America's] critical infrastructure—our financial systems, our power grid, health systems—run on networks connected to the Internet, which is hugely empowering but also dangerous, and creates new points of vulnerability that we didn't have before. (Obama)

Indeed, successful cyber-attacks on computer systems that control major infrastructure could cripple the nation. Patrick T. Hemmer considers the ramifications of a successful large-scale cyber-attack on infrastructure: "Supervisory control and data acquisition systems (SCADA) that control the functions of power, nuclear, sewer, and air defense systems (among others) could either be crippled or engineered to create massive nuclear and biological emergencies" (28). Hemmer goes on to state that "government attempts to counter or defend against an attack of this nature would be limited and piecemeal" (28). The cyber-attack situation described by Hemmer could have a devastating toll on the military and civilian population of the targeted nation. This is particularly concerning due to the strong correlation that exists between a

country's level of technological development and its vulnerability to such cyber-attacks. This correlation implies that the world's major countries are also the most vulnerable. David E. Sanger of *The New York Times* concluded that "no country's infrastructure is more dependent on computer systems, and thus more vulnerable to [cyber-attack], than that of the United States" (Sanger).

As such, the development of major cyber weapons by developed nations could in fact pose a similar situation to that of the nuclear arms race of the Cold War; developed nations could use cyber weapons as deterrents. The idea is that if one country initiates attack, the other will respond in kind, thus resulting in "mutually assured destruction"—a political doctrine that characterized Soviet-American relations during the Cold War (de Castella). At first glance, this theory fits perfectly; cyber weapons do indeed have vast destructive capabilities, and President Obama has already referred to the field of cyber security as a "cyber arms race" (Obama). However, there are a few critical differences between cyber weapons and nuclear weapons that make them particularly dangerous to world peace.

Unlike nuclear weapons during the Cold War, cyber weapons can also be developed by groups or people who are not affiliated with a government, which creates the potential for cyber terrorism. As early as 1991, a report by the National Research Council recognized that "tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (7). Furthermore, cyber weapons allow the user to leverage "anonymity and deniability while conducting military campaigns in cyberspace" (Wilson); this makes it difficult to verify the origin of an attack and thus poses less risk of retaliation to the user. This shield of anonymity—a weapon-trait that is not possessed by nuclear weapons—weakens the political doctrine of mutually assured destruction. After all, how can you retaliate against an enemy that you can't even identify? When combined, these two attributes can create a very tense climate between major world powers: Not only is the promise of mutually assured destruction a less effective deterrent, but there are also more potential sources of attack. This tension can be worsened by another attribute of cyber weapons that is summarized by Hemmer: "Specific capabilities of [cyber weapons]… are closely guarded secrets. As such, it is very likely that an adversary forms a potentially uneducated opinion as to the effectiveness of their defenses" (20). This fear of inadequate defenses could theoretically push major nations to develop more advanced weapons and defenses, thus fueling a cyber arms race. Together, these factors would create a more volatile political climate with a higher potential for significant destruction.

The thought of a future cyber war is certainly a frightening one. Cyber weapons have enormous potential for destruction and, as we have seen, have qualities that make them especially hazardous to world peace when used as militaristic weapons. It appears, though, that world leaders are aware of the potential risks of such weapons, at least to a certain extent. For example, when questioned about why he has not employed cyber weapons against political targets like China and North Korea, President Obama "has repeatedly told his aides that there are risks to using—and particularly to overusing—the [cyber weapon]" (Sanger). President Obama's restraint regarding the use of cyber weapons shows that he is aware of the risks that such weapons carry. Namely, it shows that President Obama aims to avoid triggering a cyber arms race between world powers, an escalation that would further agitate an already tense political climate and could potentially lead to destruction on a massive scale. On the other hand, there is a great deal of concerning evidence suggesting that international affairs may indeed be pushing the world towards a cyber war. In "Stuxnet and the Future of Cyber War," Farwell and Rohozinski point out that "the United States views cyberspace as a war-fighting domain that favours offense. Its policy explicitly seeks superiority in that domain" (Farwell and Rohozinski). This approach to cyber space resembles the deterrent-based diplomatic approaches that characterized and fueled the nuclear arms race of the Cold War. More worryingly, recent cyber-attacks have already strained the relationship between the United States and other major world powers. At the beginning of October, for example, the United States accused Russia of meddling with the upcoming presidential election by hacking the Democratic National Committee's computers—a cyber-attack that Russia is vehemently denying involvement in. On the matter, Senator Ben Sasse

has expressed his belief that the United States must respond with "a strong diplomatic, political, *cyber* and economic response" (qtd. in Nakashima). Equally troubling is that Iran has responded to the Stuxnet attack by forming a military cyber unit that is similar in purpose to that of the United States Cyber Command. On the matter, "Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared 'to fight our enemies' in 'cyberspace and Internet warfare'" (qtd. in Sanger).

While computer systems and cyber space have allowed us to vastly improve nearly every aspect of human existence, they have also left us with an existential crisis. The more we incorporate technology into real-world processes, the more we put ourselves at risk of serious cyber-attacks. As President Obama put it, "it's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm" (Obama). What remains clear is that the future role of cyber weapons in political and military affairs is largely uncertain and remains dynamic. Going forward, we can only hope that major world leaders consider the tremendous implications of cyber weapons and cyber warfare when conducting diplomacy. After all, the cyber weapon may very well be the greatest revolution in weapon technology since the Manhattan Project.

Works Cited

de Castella, Tom. "How Did We Forget about Mutually Assured Destruction?" *BBC News*, 15 Feb. 2012, www.bbc.com/news/magazine-17026538. Accessed 31 Oct. 2016.

Farwell, James P., and Rohozinski, Rafal. "Stuxnet and the Future of Cyber War." *Survival*, vol. 53, no. 1, 2011, pp. 23-40.

Hampson, Noah C.N. "Hacktivism: A New Breed of Protest in a Networked World." *Boston College International and Comparative Law Review*, 6th ser., vol. 35, no. 2, 2012, pp. 511-42. *SSRN*. Accessed 30 Oct. 2016.

Hemmer, Patrick T. *Deterrence and Cyber-weapons*. Dissertation, Naval Postgraduate School, 2013. Accessed 30 Oct. 2016.

Langner, Ralph. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security and Privacy*, vol. 9, no. 3, 2011, pp. 49-51.

Nakashima, Ellen. "U.S. Government Officially Accuses Russia of Hacking Campaign to Interfere with Elections." *The Washington Post*, 7 Oct. 2016, www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.3bf9632c6d48. Accessed 28 Oct. 2016.

National Research Council. "Overview and Recommendations." *Computers at Risk: Safe Computing in the Information Age*. The National Academies Press, 1991.

Obama, Barack. "Remarks by the President at the Cybersecurity and Consumer Protection Summit." Cybersecurity and Consumer Protection Summit, 13 Feb. 2015, Stanford University, Stanford, CA. Accessed 30 Oct. 2016.

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times*, 1 June 2012, www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Accessed 30 Oct. 2016.

Wilson, Clay. "Cyber Weapons: 4 Defining Characteristics." *GCN*, 4 June 2015. Accessed 29 Oct. 2016.

Winterfeld, Steve, and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Syngress, 2012.