National Security Policy, Technology and Cyber

Oscar Hernandez Mata

How does cyber as a new technology compare with earlier technological innovations that affected national security and international relations? Are the emerging strategies and political challenges fundamentally similar or different for cyber as compared with other new technologies?

Raymond Bauer states that technology emerges from society to solve an initial problem, which most of society's members have decided by mutual agreement. The solution process starts as "purely technical" (Bauer 1969, 14), not involving policy. However, the creation of technology has consequences that might not be desirable, visible, or understood at first (Bauer 1969, 15). These consequences are usually of a more considerable magnitude. Thus, technology is perceived as the engine that makes society move since innovations have major consequences that can drastically transform societies (Bauer 1969, 14-18).

New technologies can emerge from sociopolitical events. Occasionally, they are not discovered, but they are built to resolve a problem or perform certain functions with a social, economic, political, or security character. In addition, events and choices can move technology in one direction instead of another, with predictable or unpredictable consequences of serious magnitude for international politics (Herrera 2006, 11). In other words, technology is a significant component of the global pollical system with the capacity to transform it.

For instance, Geoffrey Herrera introduced the theory of the pike and its contribution to the end of feudalism and the transformation of the premodern era to the modern. The Swiss mercenaries were masters of using the pike for defense purposes. However, the Europeans adapted the Swiss method and turned it into the "modern army of pike and gun" (Herrera 2006, 1). The success of the pike

practice by the French over the traditionally mounted knights led other European states to rethink their security policies, conquest strategies, and behaviors (Herrera 2006, 2).

On the other hand, atomic science was a product of a state-funded German policy, which allowed universities to monopolize scientific research during the early XX century. This policy aimed to elevate Germany's international prestige, make it more competitive internationally and develop it economically. The discovery of X-rays by Wilhelm Conrad Röntgen in 1895 marked the beginning of the field of nuclear physics. Subsequently, in the 1930s, atomic research intensified with the discovery of nuclear fission by German scientists Otto Hahn and Fritz Strassmann in 1938, which eventually led to the development of the nuclear bomb (Herrera 2006, 130).

When the nazis took over Germany and invaded Europe, many Jewish scientists were expelled from the universities and forced to migrate. The United States benefited from the immigration of this scientific talent. Without these immigrants, the creation of the atomic bomb and the development of nuclear energy would have been delayed. Besides, using the former at the end of WWII would not have occurred (Herrera 2006, 118). Hence, the atomic bomb and the subsequent development of nuclear power were a product of the scientific capacity in the United States, historical events (WWII), and political forces[1]. This new technology altered the states' interaction capacity by modifying the international system and created new threats and challenges for governments.

As innovations emerge, governments are forced to implement new regulations and policies to prevent external and internal threats that could arise from new technologies. For example, the nuclear bomb and nuclear energy development impacted policies in various governmental areas

[1] Note: The US government financed the research of the atomic bomb development during WWII.

such as energy, environmental, and national security. In addition, nuclear and radiological attacks by terrorist groups became a fundamental national security policy concern for the United States after the collapse of the Soviet Union and later the 9/11 attacks.

The 9/11 tragic events transformed the United States' national security policies. The government realized that America was vulnerable to internal attacks, especially from non-state actors. Many questions arose after the 9/11. What if a terrorist organization created a nuclear or radiological weapon and detonated it in a major American city? There was evidence that Osama Bin Laden intended to create a weapon of mass destruction and detonate it in U.S territory. The U.S. government responded to these new technological threats through policies that created offices within the Department of Homeland Security responsible for conducting research, development, testing, and evaluating nuclear and radiological detection technologies. For instance, the Domestic Nuclear Detection Office's (DNDO) task was to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport radiological or nuclear material for use against the U.S. The DNDO also provided standardized threat assessments, technical support, training, and response protocols for federal and non-federal partners (Department of Homeland Security (D.H.S.), 2007).

From 2004 to 2023, nuclear terrorist policies did not drastically change. The different administrations maintained the main target of creating technologies to secure points of entrance to the U.S. and detect risky nuclear and radiological devices. During the George W Bush administration, the D.H.S. started creating technological projects to be deployed at US Ports-of-Entry and critical points in the intermodal transportation system. Subsequently, during the Obama, Trump, and Biden administrations, the technologies evolved from testbed projects and advanced detector prototypes to the completion and deployment of radiation and nuclear detection

equipment such as personal radiation detectors, handheld Radio-Isotope Identification Devices, backpack detectors, and Linear Radiation Monitors for Customs and Border Protection. Besides, these administrations were responsible for the protection against nuclear terrorism expansion to more than 100 northern land border crossings, thanks to the Northern Border Initiative, which has deployed radiation detection portals to ensure 100% scanning of cargo and personal transport at the Northern Border (D.H.S., 2005-2022).

The U.S. policies to protect Americans against nuclear terrorism go beyond detecting and preventing radiation and nuclear weapons from coming into the country. These policies also focus on keeping the cities safe. For example, the administrations mentioned above have provided counter-radiation and nuclear resources to high-risk metropolitan regions like New York City to reduce the risk of a successful movement or deployment of radiation and nuclear weapons of mass destruction in those cities. On the other hand, through the NNSA, the government conducts operations to protect major public events from nuclear or radiological threats by performing aerial surveys before significant events to establish a baseline measurement of natural background radiation (National Nuclear Security Administration, 2023).

As the pike and nuclear cases, the invention of the internet transformed the world by connecting people and making information accessible in unprecedented ways. It also facilitated the flow of products and services globally, thus, becoming indispensable in people's daily lives. However, this heightened connectivity has also prompted new cybersecurity risks and challenges with far-reaching implications. Hence, the United States government has created policies that address the risks linked to cyberspace.

The Obama administration acknowledged that in cyberspace, people can be victims of extortion, fraud, and theft. Among its fundamental concerns were the theft of intellectual property that could

jeopardize the U.S. competitiveness and innovations, the international peace and security that could be threatened by conventional conflict mechanisms that extended into the cyberspace (The White House 2011, 4), cyberattacks perpetrated by foreign governments, terrorist organizations, criminal groups or people on their initiative committing espionage, making a political statement or voicing personal dissatisfaction (Department of Defense (D.O.D.) 2011, 3).

Another primary fear regarding cybersecurity lies in software and hardware. According to the Department of Defense in the United States, most information technology products are produced abroad, which represents a challenge for the D.O.D. when managing risks in their design, production, service, distribution, and discarding (D.O.D. 2011, 3).

Cyber threats to U.S. national security extend beyond the military to all parts of society. Advanced hackers and foreign governments have become more skilled at infiltrating the networks and systems that regulate essential civilian infrastructure. With cyberspace being so interconnected, failures in power grids, transportation networks, or financial systems caused by computer malfunctions could lead to significant destruction and economic turmoil. Besides, the operations carried out by the D.O.D., both domestically and overseas, rely on this vital infrastructure (D.O.D. 2011, 4).

In order to counterattack these risks, the U.S. government developed cybersecurity policies that targeted states' respect for the free flow of information whenever it did not interfere with internationally interconnected infrastructure (The White House 2011, 10). Additionally, these policies have focused on organizing, training, and equipping people at all levels for the challenges and opportunities of cyberspace. Furthermore, they also promote the practice of cyber hygiene, that is, to keep security software and operating systems updated. Recently, U.S. cybersecurity policies have established cooperation and partnership between the U.S. government departments

and agencies and the private sector to enable a whole-of-government cybersecurity strategy. Also, cybersecurity cooperation has extended beyond the domestic sphere to U.S. allies and international partners, specifically NATO members (D.O.D. 2011, 5-10).

Some policy analysts consider that traditional deterrence policy is effective in regard to dissuading enemies from conducting cyberattacks against the United States. However, this might not be the case. If, during Cold War times, threats of retaliation to nuclear attacks by using atomic weapons effectively worked in the cybersecurity realm, military force cannot be used every time there is a cyberattack. First, the United States' dependence on cyber connectivity makes it vulnerable and a constant target. Second, cyberattacks might be carried out by unknown adversaries, making punishments based on military force a reasonable strategy as it does for nuclear weapons (Nye 2017, 55).

Joseph Nye Jr states that cyberspace has four ways to reduce cyberattacks: "threat of punishment, denial by defense, entanglement, and normative taboos (Nye 2017, 54)." Deterrence by denial is currently one of the most important cybersecurity strategies. A good cyber defense can reduce incentives for cyberattacks by making them look pointless. Keeping a strong cyber defense can protect essential infrastructures and industries. Thus, investments in resilience can improve deterrence in cyberspace (Nye 2017, 56).

For some scholars, the offense-defense balance in cyberspace is formed by the skills adversaries possess to handle complex information technology and the difficulty of their objectives (Slayton 2016-2017, 74). However, according to Saltzman, the balance between offense and defense in cyberspace is stated traditionally: "mobility enhancement and firepower's degree of destructiveness" (Saltzman 2013, 43). Regardless of the approach, adjusting the work factor of offense and defense is a way to implement deterrence by denial effectively. For instance,

consuming the attacker's resources can increase the costs and ultimately deter attacks. Besides, as mentioned above, good cyber hygiene forced by governments can enhance deterrence by denial (Nye 2017, 57).

Besides punishment and denial, entanglement is another mechanism to make an actor deter from committing a cyberattack. The concept of entanglement pertains to multiple interdependencies that cause a successful attack, resulting in significant consequences for both the perpetrator and the target. If the status quo remains intact, adversaries will be persuaded to attack because they might lose valuable benefits (Nye 2017, 58).

The last tool of deterrence is norms and taboos. Normative considerations can harm reputations, damaging an actor's soft power. This damage can surpass the value obtained from the attack. Norms can cause costs for an attacker, especially when the state that attacks do it against a weaker actor. This violates shared accepted standards and undermines the attacker's soft power of attraction (Nye 2017, 60).

If we compare nuclear weapons policies during the 1950s and cybersecurity, nuclear weapons were considered "standard" weapons. However, since nuclear weapons were not used, the norm of not using them became accepted. Thus, states consider the cost of using nuclear weapons before deciding. Many years of nonuse of atomic weapons have had a preventive outcome. In the cybersecurity realm, it is not about weapons but about targets. The U.S. and the international community have approved international laws of armed conflict, which ban attacks on civilians, including those concerning cyberspace. "A state should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public (Nye 2017, 61)."

In conclusion, the Unites States' cybersecurity and nuclear policies involve using advanced technology to protect its national security interests. In addition, they apply defensive strategies that require adaptations to threats and technologies. Furthermore, these policies demand coordination and communication between agencies, departments, and civilian authorities. However, cyberattacks are usually less catastrophic than nuclear attacks, although they can significantly destroy infrastructure and lose data. On the other hand, nuclear weapons are regulated by strict international laws, whereas cyber weapons are more recent, with norms that are not as well formulated as nuclear weapons' rules. Using atomic weapons is more limited than cyber-attacks, which states and non-state actors can conduct.

References

Bauer, R. A. (1969). *Second Order Consequences of Tech: A Methodological Essay on the Impact of Technology.* The M.I.T Press.

Bunn, M. (2009). Reducing the Greatest Risk of Nuclear Theft & Terrorism. *Deadalus, 1*(4), 112-123.

Diez, E., Clark, T., Zaw-Mon, C., (2010). Global Risk of Nuclear Terrorism. *Journal of Strategic Security, 3*(1), 19-30.

Herrera, G. (2006). *Technology and International Transformation. The Railroad, The Atom Bomb, and the Politics of Technological Change.* New York: State University of New York Press.

Department of Defense United States. U.S Department of Defense. (2011). Strategy for Operating in Cyberspace.

Homeland Security United States. U.S Department of Homeland Security. (2004). Budget-in-Brief: Fiscal Year 2004.

Homeland Security United States. U.S Department of Homeland Security. (2005). Budget-in-Brief: Fiscal Year 2005.

Homeland Security United States. U.S Department of Homeland Security. (2006). Budget-in-Brief: Fiscal Year 2006.

Homeland Security United States. U.S Department of Homeland Security. (2007). Budget-in-Brief: Fiscal Year 2007.

Homeland Security United States. U.S Department of Homeland Security. (2008). Budget-in-Brief: Fiscal Year 2008.

Homeland Security United States. U.S Department of Homeland Security. (2009). Budget-in-Brief: Fiscal Year 2009.

Homeland Security United States. U.S Department of Homeland Security. (2010). Budget-in-Brief: Fiscal Year 2010.

Homeland Security United States. U.S Department of Homeland Security. (2011). Budget-in-Brief: Fiscal Year 2011.

Homeland Security United States. U.S Department of Homeland Security. (2012). Budget-in-Brief: Fiscal Year 2012.

Homeland Security United States. U.S Department of Homeland Security. (2013). Budget-in-Brief: Fiscal Year 2013.

Homeland Security United States. U.S Department of Homeland Security. (2014). Budget-in-Brief: Fiscal Year 2014.

Homeland Security United States. U.S Department of Homeland Security. (2015). Budget-in-Brief: Fiscal Year 2015.

Homeland Security United States. U.S Department of Homeland Security. (2016). Budget-in-Brief: Fiscal Year 2016.

Homeland Security United States. U.S Department of Homeland Security. (2017). Budget-in-Brief: Fiscal Year 2017.

Homeland Security United States. U.S Department of Homeland Security. (2018). Budget-in-Brief: Fiscal Year 2018.

Homeland Security United States. U.S Department of Homeland Security. (2019). Budget-in-Brief: Fiscal Year 2019.

Homeland Security United States. U.S Department of Homeland Security. (2020). Budget-in-Brief: Fiscal Year 2020.

Homeland Security United States. U.S Department of Homeland Security. (2021). Budget-in-Brief: Fiscal Year 2021.

Homeland Security United States. U.S Department of Homeland Security. (2022). Budget-in-Brief: Fiscal Year 2022.

Homeland Security United States. U.S Department of Homeland Security. (2023). Budget-in-Brief: Fiscal Year 2023.

National Nuclear Security Administration. (n.d). *Counterterrorism and Counter Proliferation.* https://www.energy.gov/nnsa/counterterrorism-and-counterproliferation.

Nye, J.S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71.

Slayton, R. (2016-2017). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. *International Security, 41*(3), 72-109.

The White House United States. U.S White House. (2011). International Strategy for Cyberspace.