The US Army War College Quarterly: Parameters

Volume 50
Number 2 *Summer 2020*

Article 6

5-15-2020

Future Warfare: Weaponizing Critical Infrastructure

Carol V. Evans

Future Warfare: Weaponizing Critical Infrastructure

Carol V. Evans

ABSTRACT: Adversaries are actively targeting US and NATO critical infrastructure, particularly energy, transportation, information, communications, and the defense industrial base sectors to undermine military capability, readiness, and force projection. In some cases, adversaries are penetrating the critical infrastructure of the United States and our allies to identify vulnerabilities for later exploitation, and in others critical infrastructure is being weaponized by Russia, China, Iran, and North Korea as a form of hybrid warfare.

The West's adversaries are using critical infrastructure (CI) as a weapon of choice in three domains.[1] First, Russia has weaponized CI in Ukraine as a testing ground for the development of larger hybrid warfare capabilities against the United States and the North Atlantic Treaty Organization.[2] Second, Russia and other adversaries have penetrated the US energy sector, particularly the US electric grid, as a means to undermine future US warfighting capabilities. Third, China has conducted strategic penetration of key critical infrastructure segments of American and European defense industrial bases. The US military and NATO have redressed these threats by investing in infrastructure resiliency based on organizational and mission capacity-building and public-private sector cooperation.

Russian Hybrid Warfare against Ukraine

The linkage between critical infrastructure as an instrument of hybrid warfare has been on open display in Georgia and the Ukraine where a Russian cyberarmy, closely affiliated with the Kremlin, has systematically attacked almost every sector of Ukraine's infrastructure for the past five years.[3] The most notable attacks included one against Ukraine's electric grid in December 2015, which left large parts of the capital city, Kiev, and the western region of Ivano-Frankivsk in the dark, and another, more technologically sophisticated attack in 2016 on one of Kiev's transmission substations. These attacks were set against the

1. This article is drawn from a larger publication by the author. Carol V. Evans, "The Economic Drivers Reshaping the International Security Landscape," in *A Changing World Order? Implications for the Security Environment*, ed. William G. Braun, Stéfanie von Hlatky, and Kim Richard Nossal (Kingston, ON: Centre for International and Defense Policy, 2020).

2. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired,* June 20, 2017, https://wired.com/story/russian-hackers-attack-ukraine/.

3. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Dr. Carol V. Evans, incoming director of the Strategic Studies Institute, US Army War College, is an adviser to the NATO Center of Excellence-Defense Against Terrorism.

backdrop of Russia's illegal annexation of Crimea in 2014 and continued military clashes in the eastern Donetsk and Luhansk regions in Ukraine.

Governments and cyberexperts attribute these cyberattacks to a Russian group known as Sandworm, which deployed its BlackEnergy malware to penetrate specialized computer architectures used for remotely managing physical industrial equipment and control systems. What most worried these cyberexperts was Sandworm had already targeted NATO networks and had compromised the computers of American and European electric and water utility companies with the same Trojan malware. This malware provided hackers with enough control to induce blackouts on American soil. As one cyberforensic expert forewarned: "An adversary that had already targeted American energy utilities had crossed the line and taken down a power grid [in the Ukraine]. It was an imminent threat to the United States."[4]

The repeated cyberattacks against Ukraine's critical infrastructure as part of Russia's hybrid warfare strategy serve Russian interests in several ways. This campaign is designed to keep Ukraine in Russia's continued orbit by thwarting Kiev's aims of integration with the European Union. Critical energy infrastructure as a tool of Russian coercion is certainly not lost on NATO and the EU. Since 2006, Russia's Gazprom has repeatedly halted gas supplies in the midst of winter to Ukraine—a vital transshipment country with pipelines to Europe—over disputes on gas pricing.

The upshot is European countries, particularly Germany, and NATO writ large are attuned to the vulnerabilities associated with their dependency on Russian gas and oil supplies. Europe could not survive 30 days without Russian gas in the winter, and its vulnerabilities will only increase with Nord Stream coming online. Certain NATO countries such as Germany are more dependent on Russian energy supplies, leading President Trump at the 2018 NATO Summit in Brussels to tweet, "What good is NATO if Germany is paying Russia billions of dollars for gas and energy?"[5]

Another rationale for Russian CI attacks in Ukraine is to test, prove, and refine Moscow's cyberwarfare capabilities against a country unable to retaliate—in essence, use Ukraine as a test bed for Russian hybrid warfare in future global conflicts, including with the United States. By turning the power off in Kiev, Moscow is both signaling and demonstrating to Washington its ability and willingness to weaponize critical infrastructure to challenge America's military might at home and overseas.

---

4. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019), 53.

5. Donald Trump (@Donald Trump), "What good is NATO if Germany is paying Russia billions of dollars for gas and energy?" Twitter, July 11, 2018, 10:07AM, https://twitter.com/realdonaldtrump/status/1017093020783710209?lang=en.

Russian Penetration of the US Energy Sector

In March 2018, the Federal Bureau of Investigation and the Department of Homeland Security confirmed Russian government hacker teams had actively "targeted government entities and multiple U.S. CI sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."[6] The Russian cyberattack teams included Sandworm, Dragonfly, and Palmetto Fusion, with some attributed with gaining remote access to actual industrial control systems and US energy sector networks including a Kansas nuclear power facility.[7] Cyberattacks against the US power grid have continued. The group Triton or Xenotime has compromised electric facility safety systems in order to cause potential plant disruption and damage. According to a researcher at the US cybersecurity firm Dragos, surveillance of the US electric grid is "indicative of the preliminary actions required to set up for a future intrusion and potentially a future attack."[8]

Penetration of the US electric grid has sounded alarm bells in the Pentagon. Department of Defense (DoD) installations and associated infrastructure depend on continuous and assured power to support missions and operations at home and abroad, and any extended loss of power has been acknowledged as a glaring national security Achilles' heel. America must expect our adversaries to disrupt the flow of power with cascading impacts on transportation, communications, and other critical infrastructure services upon which the US military depends. After all, for decades the former Soviet Union carefully studied the US homeland and its warfighting infrastructure for infiltration and targeting purposes.

The game changer for today, however, is that with cyberspace and the merging of CI with information and communications technologies, our adversaries no longer require kinetic solutions and direct military confrontation with the United States. Rather as one senior DoD official conceded, "the smart thing to do is to maneuver around those forces, attack the critical infrastructure, the facilities here in the United States on which we depend to deploy, operate and sustain our forces abroad."[9]

The willingness and ability of our adversaries to deploy destructive cyberweapons in future warfare with the United States has immense national security implications. Of immediate concern is the threat to deterrence and intrinsic force projection capabilities—"it does not matter how capable, how well trained or how advanced a nation's forces

6. Cyber and Infrastructure Security Agency (CISA), US Department of Homeland Security (DHS), "Alert TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," DHS, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

7. John Kennedy, "US Officially Blames Russia's 'Dragonfly' Hackers for Attacks on Energy Grid," Silicon Republic, March 26, 2018, https://www.siliconrepublic.com/enterprise/dragonfly-us-russia-energy-grid-hackers.

8. Andy Greenberg, "The Highly Dangerous 'Triton' Hackers Have Probed the US Grid," *Wired*, June 14, 2019, https://www.wired.com/story/triton-hackers-scan-us-power-grid/.

9. Paul Stockton cited in Cynthia E. Ayers and Kenneth D. Chrosniak, *Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency*, Issue Paper 1-13 (Carlisle Barracks, PA: US Army War College, October 2013), CSL-5.

are if they can't get to the front in time."[10] The deliberate targeting of civilian infrastructure has larger security and ethical implications which have yet to be addressed fully.[11]

Chinese Investments in the United States and Europe

"China, in particular, has made it a national goal to acquire foreign technologies to advance its economy and to modernize its military. . . . It is comprehensively targeting advanced US technologies and the people, the information, businesses and research institutions that underpin them."[12] To achieve this national goal, China has used an effective combination of industrial, trade, and investment policies.

Initiated in 2015, Beijing's Made in China 2025 industrial policy directs Chinese technological development in important dual-use areas: artificial intelligence, quantum computing, robotics, aerospace, autonomous and new energy vehicles, communications, and other emerging industries. China analysts have focused largely on the government's illicit means to acquire these technologies through espionage, cyberoperations, evasion of US export control restrictions, and through coercive intellectual property sharing requirements for foreign companies investing in the Chinese market. Less attention has been paid to Beijing's "Go Out" strategy of promoting Chinese state-owned and private sector champions to invest overseas, particularly in the United States and Europe, in key defense industrial base sectors. Outward foreign investments and acquisitions have been assisted by Beijing-backed investment vehicles, such as the China Investment Corporation and massive sovereign wealth funds.[13]

This inattention changed dramatically with the recent bid by Chinese tech giant Huawei to provide 5G information and communications technology networks in the United States and Europe. The case of Huawei poses a number of concerns for the security of the defense industry base in the United States and Europe. For example: Should the United States and Europe be dependent on China to provide a key, dual-use defense industry base infrastructure? Through its control of the world's wireless and telecommunications backbone, will the Chinese government use 5G as a Trojan horse for commercial and military espionage and hybrid warfare purposes?

---

10. Omar Lamrani, "Why Logistics Will Be the Key to Any U.S. Conflict with Russia and China," Worldview, Stratfor, December 17, 2018, https://worldview.stratfor.com/article/why-logistics-will-be-key-any-us-conflict-russia-and-china/.

11. Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser, eds., *Binary Bullets: The Ethics of Cyberwarfare* (New York: Oxford University Press, 2016).

12. *Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense: Hearing before the House Armed Services Committee*, 115th Cong. (June 21, 2018) (statement of Kari A. Bingen, Deputy Undersecretary of Defense for Intelligence), https://armedservices.house.gov/hearings?ID=FAC043FA-B7E9-4E08-A2A7-226F7DA5D8F8.63.

13. White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World* (Washington, DC: White House Office of Trade and Manufacturing Policy, June 2018).

The response by the Trump administration to Huawei has been swift and decisive. It has banned Huawei from all federal contracts for telecommunications equipment and services, and US government contractors are prohibited from doing business with Huawei as well.[14] The US Department of Justice filed formal charges of fraud, obstruction of justice, and theft of trade secrets against Huawei in January 2019. Additionally, the administration has exerted considerable pressure on its partners within the Five Eyes intelligence alliance to ban Huawei from their respective markets.

Concerned about the larger implications of Chinese investments and other adversarial activities involving the US defense industry base infrastructure, Congress passed the Foreign Investment Risk Review Modernization Act of 2018 as part of the larger National Defense Authorization Act of 2019. This legislation expands the powers of the Committee on Foreign Investment in the United States to prevent foreign adversaries from gaining control of defense industrial infrastructure assets.[15] That same year, the Trump administration issued Executive Order 13806, which mandated an assessment of US defense industry base. This assessment concluded, "all facets of the manufacturing and defense industrial base are currently under threat, at a time when strategic competitors and revisionist powers appear to be growing in strength and capability."[16]

European countries have been slow to recognize the potential security vulnerabilities and dependencies created by Chinese investments in infrastructure. China has launched the 17+1 Initiative, a forum under Beijing's larger Belt and Road Initiative, that includes 12 EU member states and five Balkan countries and provides major infrastructure loans for the construction of high-speed rail networks, port infrastructure, communications, bridges, and highways. Chinese companies have acquired shipping terminals in Spain, Italy, and Belgium. Major Chinese port infrastructure projects include the Italian ports of Trieste, Venice, and Ravenna, as well as the Greek port of Piraeus, Koper in Slovenia, and Fiume in Croatia. In October 2019, Germany's Chancellor Angela Merkel allowed Huawei and ZTE (also Chinese-owned) greater market access into this key NATO ally's 5G networks. This decision has multiple international security implications—it threatens NATO security and

14. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018); and US Federal Communications Commission (FCC), *Protecting against National Security Threats to the Communications Supply Chain through FCC Programs*, FCC 19-121 (Washington, DC: FCC, November 26, 2019), https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0.

15. Pub. L. No. 115-232, § 1701(c).

16. US Government Interagency Task Force, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States: Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806* (Washington, DC: Department of Defense [DoD], September 2018), 8.

the operations of the US military presence based in Germany, and it contravenes US intelligence warnings.[17]

Chinese involvement in key infrastructure projects in Europe has garnered increasing concern by NATO regarding Beijing's intentions and the need for a shared Allied policy on China. On the occasion of NATO's 70th anniversary meeting in London in December 2019, Secretary General Jens Stoltenberg warned: "What we see is that the rising power of China is shifting the global balance of power. . . . We have to address the fact that China is coming closer to us, investing heavily in infrastructure. . . . So, of course, this has some consequences for NATO."[18]

A recent NATO report was more direct in identifying the potential consequences of the penetration of defense industry base infrastructure by adversaries on NATO security. "The degree and impact of foreign direct investment in strategic sectors—such as airports, sea ports, energy production and distribution, or telecoms—in some Allied nations raises questions about whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military."[19]

As with issues of energy security, NATO is grappling with dependency on European host-country infrastructure and the vulnerabilities this poses for logistics, secure communications, and other requirements to enable mobilization, force projection, and sustainment.

Arguably, Chinese Belt and Road Initiative investments in Europe are part of a deliberate strategy by Beijing to target economically weaker NATO members to draw them into China's orbit. Indeed, this strategy appears to be having some success. Hungary and Greece sought to block any direct reference to China in an EU statement regarding the ruling by the Permanent Court of Arbitration in The Hague that struck down the People's Republic of China's legal claims in the South China Sea.[20]

Sounding the alarm over the long-term implications of European Belt and Road Initiative investments on EU unity, Germany's foreign minister forewarned, "if we do not succeed for example in developing a single strategy towards China, then China will succeed in dividing Europe."[21] Incremental progress has been made recently with a new

17. John R. Deni, "Germany's Refusal to Ban China's Huawei from 5G is Dangerous for the West," *Newsweek*, October 30, 2019, https://www.newsweek.com/germanys-refusal-ban-chinas-huawei-5g-dangerous-west-opinion-1468520.

18. Holly Ellyatt, "China is 'Coming Closer' but We Don't Want a New Adversary, NATO Chief Says," CNBC, December 2, 2019, https://www.cnbc.com/2019/12/02/jens-stoltenberg-rising-power-china-must-be-addressed-by-nato.html.

19. Wolf-Diether Roepke and Hasit Thankey, "Resilience: The First Line of Defense," *NATO Review*, February 27, 2019, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

20. Erik Brattberg and Etienne Soula, "Europe's Emerging Approach to China's Belt and Road Initiative," (Washington, DC: Carnegie Endowment for International Peace, October 19, 2018), https://carnegieendowment.org/2018/10/19/europe-s-emerging-approach-to-china-s-belt-and-road-initiative-pub-77536.

21. Lucrezia Poggetti cited in Peter Frankopan, *The New Silk Roads: The Present and Future of the World* (New York: Alfred Knopf, 2019), 172.

EU regulation establishing a framework for screening foreign direct investments in critical infrastructure and technologies. This new regulation is due to come into full effect in November 2020.[22]

Redressing CI Vulnerabilities

Beginning in 2005, the DoD initiated an enterprise-wide Defense Critical Infrastructure Program which focused on identifying key defense infrastructure assets and developing guidelines and procedures for their protection.[23] With the launch in 2012 of the Department's Mission Assurance Strategy, the focus shifted from protecting defense critical assets toward *strengthening the resiliency of DoD missions*. Mission Assurance is "a process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the performance of DoD MEFS [mission essential functions] in any operating environment or condition."[24]

Recognizing over 90 percent of US infrastructure resides in the private sector, the Mission Assurance Strategy also called for strengthening DoD partnerships with those commercial infrastructure owners and operators. The strategy has been augmented by other policy directives that require and provide all services, departments, and agencies with guidelines for identifying, assessing, managing, and monitoring risks to strategic missions.[25]

In contrast to the deliberate process of the US military, NATO has taken a less structured approach to redress critical infrastructure vulnerabilities. Its initial efforts focused on building organizational capacity with the establishment of NATO Centres of Excellence (COE) to support CI protection: Defense Against Terrorism-COE (Turkey), Cooperative Cyber Defense-COE (Estonia), Energy Security-COE (Lithuania). These centers have been bolstered by the work of the European COE for Countering Hybrid Threats (Finland).

The targeting of civilian infrastructure as part of Russia's hybrid warfare in Ukraine further spurred NATO efforts, in cooperation with the EU, to enhance critical infrastructure resiliency through developing baseline requirements for measuring and improving civil preparedness.[26] Additional mitigation measures include the deployment of cyber and hybrid warfare support teams, enhanced information-sharing with

22. High Representative of the Union for Foreign Affairs and Security Policy, European Commission, "Joint Communication to the European Parliament, The European Council and the Council: EU-China—A Strategic Outlook," European Commission, March 12, 2019, https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.

23. Assistant Secretary of Defense (Homeland Defense), *Defense Critical Infrastructure Program*, DoD Directive (DODD) 3020.40 (Washington, DC: DoD, August 19, 2005); and Office of the Undersecretary of Defense (Policy) (OUSD[P]), *Defense Critical Infrastructure Program (DCIP) Management*, DoD Instruction 3020.45 (Washington, DC: OUSD(P), April 21, 2008).

24. OUSD(P), *Mission Assurance Strategy* (Washington, DC: DoD, April 12, 2012), 1, https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf.

25. Assistant Secretary of Defense (Homeland Defense), *Critical Infrastructure Program*.

26. Roepke and Thankey, "First Line of Defense."

the EU and the private sector, and the integration of energy and cyberinfrastructure requirements within NATO exercises—Locked Shields 2018—and war games.

Conclusion

The use of critical infrastructure as a weapon by our adversaries has received little attention in international security circles. As discussed previously, CI can be used as an instrument of hybrid warfare among weaker states such as Ukraine and against superpowers such as the United States. Whether through the use of cyberattacks against a country's infrastructure, or more covertly through surveillance and penetration, or via acquisitions and direct foreign investment, targeting of critical infrastructure enables our adversaries to shape and control vital defense industry base infrastructure upon which US and NATO militaries rely.