State: Ukraine
Threat: Cybersecurity Vulnerabilities and Nuclear Infrastructure

The following brief was prepared to assess the threat of potential cyberattacks on Ukrainian nuclear energy infrastructure and provide some mitigation strategies.

I. Introduction

The country of Ukraine has been the victim of several of the world's largest and most devastating cyber attacks in the last decade. Indeed, Ukraine was the target of what is considered the most extensive attack in history – the NotPetya incident of June 2017. This incident solemnly emphasizes the need for a review of Ukraine's cybersecurity policy and its intersection with nuclear security. In fact, the NotPetya attack even reached the radiation monitoring systems in the Chernobyl Exclusion Zone, forcing staff to conduct the protocols manually.[1] While the spread of the 2017 ransomware was rather indiscriminate in nature, it caused devastation in the systems of various Ukrainian government agencies, multinational corporations and touched our nuclear infrastructure.[2] This demonstrates how cyberweapons are an evolving, emerging threat in the nuclear domain and how Ukraine in particular might position itself for enhanced defense on this front.

II. Nuclear Security – A Foundational Pillar of International Obligations

Ukraine has been a member of the International Atomic Energy Agency (IAEA) since July 1957 and is subject to a number of provisions of the Agency.[3] One of the three pillars of the IAEA along with safeguards is "Safety and Security". As part of this, the IAEA itself addressed the importance of cybersecurity in a June 2015 conference stating that, *"Regulation must address information technology systems, industrial control systems and physical protection systems used within the nuclear industry"*[4] and that the IAEA and the member states therein must take initiative in these endeavors. Given Ukraine's international obligations, it is imperative that both the government and the private sector explore avenues for mitigating the threat of cyberattack and/or intrusion in its nuclear sector.

III. General Threat Landscape

Prior to exploring the threat landscape specific to the Ukrainian context, it is important to give a broad overview of the threat of nuclear cybersecurity vulnerabilities more generally and why it is a concern for the next decade. Research has been done on cyber vulnerabilities for both peaceful and military nuclear capabilities. While it is not the focus of the current brief as Ukraine does not possess nor produce nuclear weapons, it is important to note that vulnerabilities in the offensive domain are a particularly troubling reality of the forthcoming decade. Given Ukraine's tenuous geostrategic positioning between Russia and NATO, disruptions in the nuclear command and control systems of Ukraine's nuclear-armed neighbors is

---

[1] Віктор Медведчук, «Кібератака добралася і до Чорнобиля». 24 Канал. Jun. 27, 2017 <https://24tv.ua/kiberataka_dobralasya_i_do_chornobilya_n835128>

[2] Patrick Reevell & Geneva Sands, "What we know about the kill switch in Petya ransomware attack". ABC News Jun. 28, 2017 <https://abcnews.go.com/International/kill-switch-petya-ransomware-attack/story?id=48324556>

[3] IAEA, Country Factsheet – Ukraine <https://ola.iaea.org/Applications/FactSheets/Country/Detail?code=UA>

[4] Rodolfo Quevenco, "Secure Computer Systems Essential to Nuclear Security, Conference Finds". IAEA. Jun. 8, 2015 <https://www.iaea.org/newscenter/news/secure-computer-systems-essential-nuclear-security-conference-finds>

an important consideration. In an excellent 2018 paper from Chatham House, the authors state that, *"Cyberattack methods such as data manipulation, digital jamming and cyber spoofing could jeopardize the integrity of communication, leading to increased uncertainty in decision-making."*[5] They also specifically mention Russia's work on a spoofing device designed to imitate jets, rockets or a missile attack to fool defense systems.[6] Both of these have serious implications for both sound decision-making for those with nuclear weapons as well as Ukraine's conventional defense systems. Rapid decision-making in nuclear weapons strategy that can be compromised by cyberweapons is a global threat and one that leaves Ukraine particularly vulnerable in its geography. This concern is compounded by the fact that many of the most potent tools to create cyberweapons are currently out in the public domain, as evidenced by the cyberweapons architecture from the infamous 2016 Shadow Broker's hack on the NSA cyberweapons cache[7] resurfacing in both the NotPetya attack in Ukraine and attacks on U.S. critical infrastructure just this month. This means that both state and nonstate actors alike have a role to play in further developing cyberweapons and evolving use typologies in coming years.

Of course, there are also major concerns with regard to the nuclear energy sector and its peaceful applications, in which Ukraine is significantly involved. The Nuclear Threat Initiative (NTI) published a report in 2019 titled *Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities*, outlining these vulnerabilities in detail. They note that terrorist groups, nation-states, ransomware hackers and "hacktivists" all have unique capabilities and motivations to carry out cyberattacks on nuclear facilities. As the authors write: *"Digital systems are integral to nuclear facilities—from enrichment facilities and reprocessing plants to spent fuel storage and nuclear power plants—throughout the fuel cycle. They perform a range of functions, including access control, materials control and accounting, and the safe and secure operation of the facility… It may be only a matter of time before the world experiences a catastrophic event… facilitated by a cyberattack deployed by a determined, well-resourced adversary."*[8] The report even highlights the 2015 attack on Ukraine's electrical grid as a case study in threats to critical energy infrastructure and note that, *"it's not inconceivable that a nuclear power plant could be attacked for similar reasons."*[9]

IV. Current Status of Ukraine

Apart from the risks posed by Ukraine's geographic positioning on the world stage, there is a robust potential for cyberattack and intrusion in the country's internal nuclear infrastructure. According to the *IAEA 2019 Annual Report*[10], Ukraine has 15 operational nuclear reactors which produced over 53% of national electricity in 2019 (see Appendix I). These reactors are located across the country and this does not include the management systems operational at the Chornobyl Exclusion Zone. Ukraine is currently in the unenviable position of having its nuclear facilities in the crosshairs of a number of different actors as

---

[5] Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences". Chatham House. January 2018. <https://stanleycenter.org/publications/other/CybersecurityofNuclearWeaponsSystemsChathamHouse.pdf>

[6] Ibid.

[7] Olivia Solon, "Hacking group auctions 'cyber weapons' stolen from NSA". The Guardian. Aug 16, 2016. <https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group>

[8] Alexandra Van Dine, et. al., "Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities". Nuclear Threat Initiative. 2019 https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf

[9] Ibid.

[10] International Atomic Energy Agency, "IAEA Report 2019" <https://www.iaea.org/sites/default/files/publications/reports/2019/gc64-3.pdf>

well as possessing more systemic risks and vulnerabilities. The 2015 attack on the electrical grid and more widespread NotPetya attack in 2017 point to the motivation of state actors (notably Russia) to seek leverage over Ukraine's energy infrastructure and with more than half of Ukraine's electricity coming from nuclear sources, the target becomes obvious. In fact, it is reported that the Cybersecurity Department of the Security Service of Ukraine neutralized over 600 cyberattacks on critical infrastructure in 2020 alone.[11] A source interviewed in a 2015 Chatham House report stated bluntly, *"I think they [Russians] have an agent in each plant; it is a priority for them to have people in Ukrainian nuclear plants."*[12] The interviewee also pointed to low wages and lack of training, motivation and English-language skills amongst CERTs (Computer Emergency Response Teams) as systemic vulnerabilities, for it leads to stale cybersecurity awareness and hampers proactivity and information-sharing. Additionally, the threat of terrorist and organized crime groups leaning on cyber means to target Ukrainian facilities remains extant. Robust trafficking networks of illicit nuclear materials have been documented right on Ukraine's border – in Georgia and Moldova, not far from the South Ukraine facility. As Dr. Beyza Unal wrote in 2015, *"The incidents in Moldova… are indicative of an expanded black market with increased demand from terrorist organizations, saboteurs and lone actors."*[13] This means that both state and nonstate actors have incentive to leverage cyber capabilities against Ukraine's active nuclear facilities as well as spent fuel storage. The NTI assessed Ukraine's general nuclear facility security capacity and ranked it 29th in the world for site protection. While Ukraine scores quite high in its "security culture", it has a medium level of cybersecurity readiness and the overall risk environment poses a myriad of challenges (see Appendix II).

V. Toolkit Available

There are a number of different avenues Ukraine can pursue in its efforts to mitigate the threat. In their aforementioned report, the NTI proposes: 1) institutionalizing cybersecurity; 2) mounting an active defense; 3) reducing complexity; and 4) pursuing transformation of cybersecurity systems by working closely with various stakeholders.[14] In the Ukrainian context, this would mean leaning on international partners, such as the IAEA, WNO, WANO and INPO and perhaps even the European Union. To begin, Ukraine should rely on the tools provided by these organizations (such as the framework outlined in *IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual: Computer Security at Nuclear Facilities*)[15], conduct targeted risk analyses at its facilities and explore areas for operationally incorporating these frameworks. It is also advisable for Energoatom (the state enterprise operating Ukraine's nuclear facilities) to foster collaboration and information-sharing between the public and private sectors. Ukraine's growing IT sector can serve as fertile soil for public-private partnerships targeted at bolstering detection and defense capabilities for the country's state-run nuclear industry. Even minor steps such as improving

[11] Promote Ukraine, "Will Ukrainian NPPs Become Target of Russia's Cyber Attacks?" Apr. 5, 2021. <https://www.promoteukraine.org/will-ukrainian-npps-become-target-of-russias-cyber-attacks/>

[12] Carolyn Baylon, et. al., "Cyber Security at Civil Nuclear Facilities: Understanding the Risks". Chatham House. Sept. 2015 <https://www.chathamhouse.org/2015/10/cyber-security-civil-nuclear-facilities-understanding-risks>

[13] Beyza Unal, "Growing Threat as Organized Crime Funnels Radioactive Materials to Terrorists". Chatham House. 13 Oct., 2015. <https://www.chathamhouse.org/2015/10/growing-threat-organized-crime-funnels-radioactive-materials-terrorists>

[14] Id 13

[15] International Atomic Energy Agency, "IAEA Nuclear Security Series No. 17, Technical Guidance Reference Manual: Computer Security at Nuclear Facilities" <https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf>

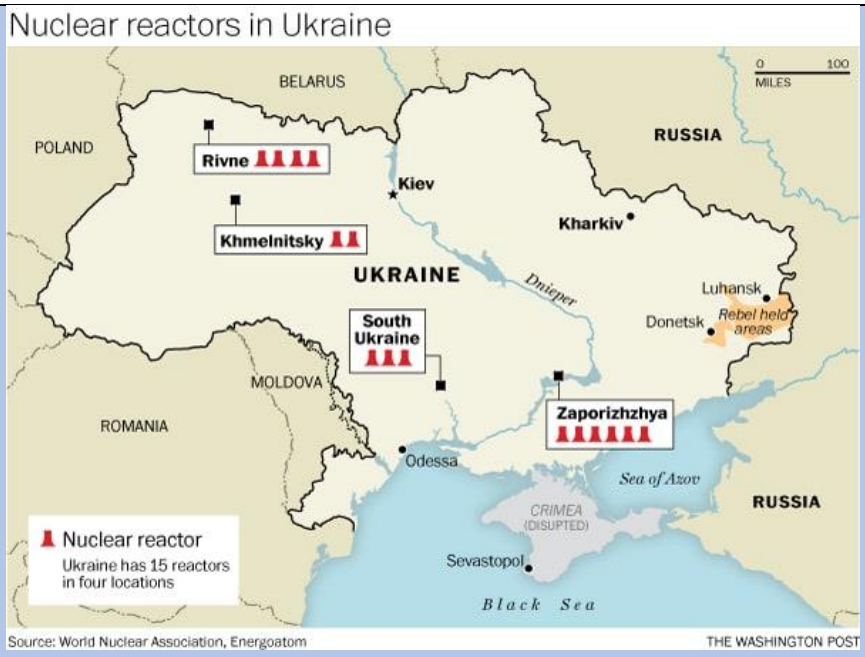
the English levels among CERTs and modernizing basic IT training within facilities would be helpful. Finally, efforts to improve security in the procurement of products used by the nuclear industry is essential. NTI insists that industry players *"demand more secure, less complex products from vendors"* and recent reports of turbogenerator excitation system software manufactured by Russia's Ruselprom being used in the South Ukrainian, Khmelnitsky and Rive power plants underscore the need for more secure procurement.[16]

While developing a toolkit in the cyber domain is a difficult task – for the toolkits of malicious actors are continually evolving in tandem – Ukraine is currently in a position to address the low-hanging fruit as well as outsource some of its toolkit crafting to its international partners.

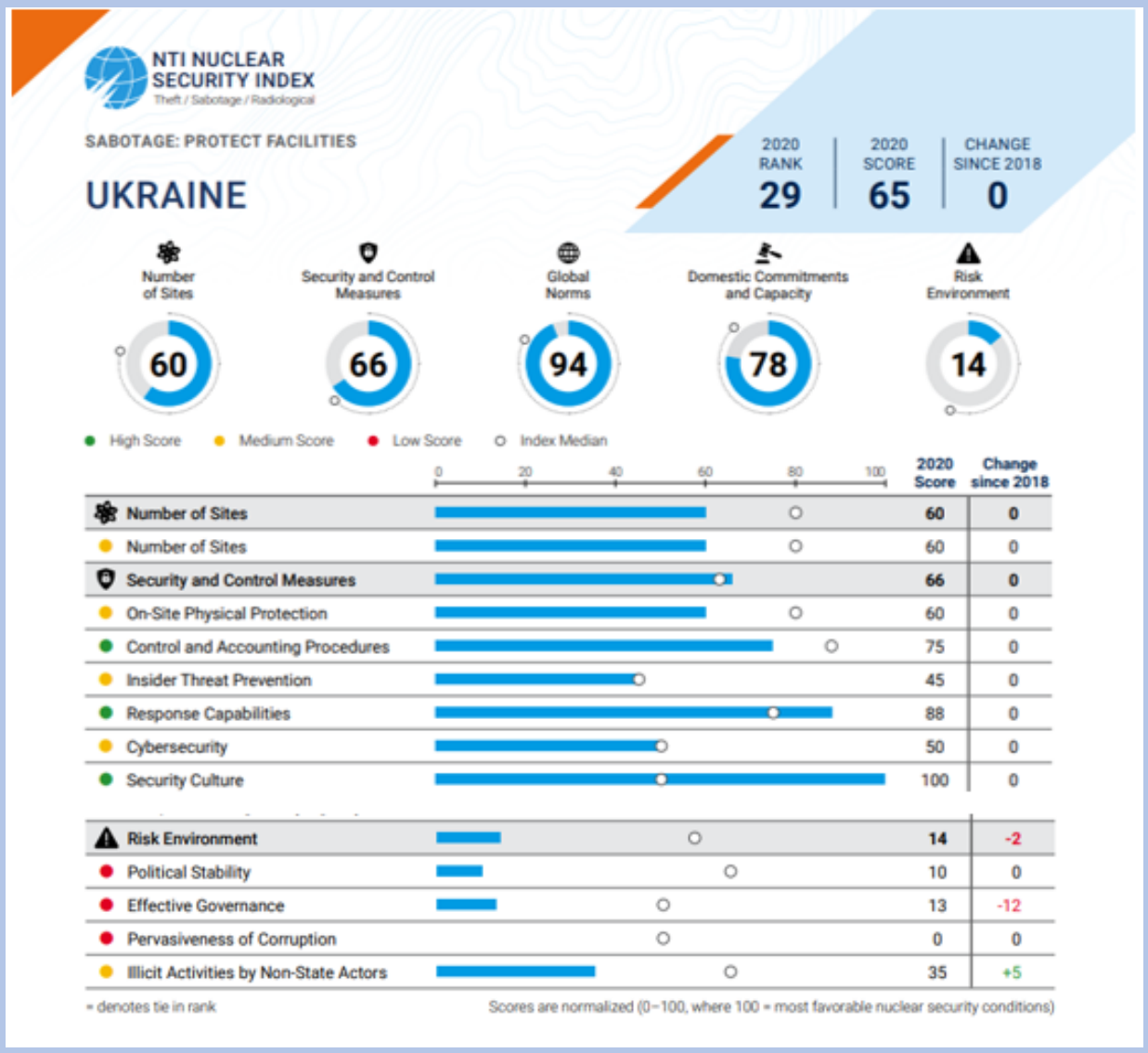
Appendix I – Current State of Ukraine's Nuclear Facilities (2020)[17] [18]

Country	Reactors in operation		Reactors under construction		Nuclear electricity supplied in 2019		Total operating experience through 2019	
	No. of units	Total MW(e)	No. of units	Total MW(e)	TW-h	% of total	Years	Months
Slovenia	1	688			5.5	37.0	38	3
South Africa	2	1 860			13.6	6.7	70	3
Spain	7	7 121			55.9	21.4	343	1
Sweden	7	7 740			64.4	34.0	467	0
Switzerland	4	2 960			25.4	23.9	224	11
Turkey			1	1 114				
Ukraine	15	13 107	2	2 070	78.1	53.9	518	6

[16] Id 16
[17] Id 15
[18] Rick Noack, "A worrying factor in Ukraine's chaos: 15 nuclear reactors". Washington Post. Sept. 3, 2014. <https://www.washingtonpost.com/news/worldviews/wp/2014/09/03/a-worrying-factor-in-ukraines-chaos-15-nuclear-reactors/>


Nuclear reactors in Ukraine
BELARUS
POLAND
RUSSIA
0
100
MILES
Rivne
Kiev
Khmelnitsky
Kharkiv
UKRAINE
Dnieper
Luhansk
Donetsk
Rebel held areas
South Ukraine
MOLDOVA
ROMANIA
Zaporizhzhya
Odessa
Sea of Azov
CRIMEA
(DISUPTED)
RUSSIA
Nuclear reactor
Ukraine has 15 reactors in four locations
Sevastopol
Black Sea
Source: World Nuclear Association, Energoatom
THE WASHINGTON POST

Appendix II – NTI Nuclear Security Index – Key Indices for Ukraine (2020)[19]



[19] Nuclear Threat Initiative, "NTI Nuclear Security Index". July 2020. https://www.ntiindex.org/wp-content/uploads/2020/09/2020_NTI-Index_Report_Final.pdf