CENTRE FOR SECURITY STUDIES | ISSUE BRIEF

August 2022

State Cyber Offensive Capabilities: A Multi-Domain Operation Construct

B. S. Ashish

Edited by: Aryan Gupta

About the author

B.S. Ashish is an undergraduate student at the Jindal School of International Affairs and a Senior Research Analyst at the Centre for Security Studies, JSIA.

About the Centre for Security Studies

The Centre for Security Studies (CSS) was established in 2020 as the Jindal School of International Affairs' first student-run research centre under the aegis of Prof Dr Pankaj K Jha. Researchers at CSS – through in-depth analysis briefs and events, reports, policy briefs and print publications – explore both regional and thematic topics in the broader field of international security studies. The concept of international security has been expanded to reflect not merely the study of state security, but also include topics like ethnic, sectarian, and religious conflict; civil wars and state failure; cyber and space warfare; resource related security issues; the proliferation of weapons of mass destruction; defence economics and also the role of ethics or morality in the formulation of security policies. The complexity of these matters is what the Centre for Security Studies attempts to unfold. Please refer to www.cssjsia.com for further details, and follow the Centre's social media platforms for critical news and research updates:

www.linkedin.com/company/jindal-centre-for-security-studies/
www.instagram.com/css_jsia/
https://twitter.com/Css_Jsia

Get in touch with us through email: css@jgu.edu.in

Important disclaimer

All views expressed in this publication belong to the author and do not reflect the opinions or positions of the Centre for Security Studies. While researchers and editors at CSS strive towards any instances, CSS as an organisation does not take any responsibility for any instance of plagiarism committed by any authors. The onus to ensure plagiarism-free work lies with authors themselves.

IB2208008

Can Cyberspace be Classified as a Domain of Warfare?

With the advent of information technology and cyber capabilities, cyberspace has been widely regarded as the 'fifth domain of warfare' in the twenty-first century. The United States Military considers cyberspace as the fifth domain of warfare- along with air, land, sea and space,[1] while China has taken into account the threats that may emanate from cyberspace while considering it as a new domain; more from a pre-emptive lens in view of China's dependence on digital economy and information technology.[2] Many other countries such as Russia, the United Kingdom, Israel, India, Australia, Japan, France, and so on, have also recognised cyberspace to be a new domain of confrontation among states.

There have been debates contesting the classification of cyberspace as a separate independent domain. To understand the debate better, the concepts of 'layers of war', 'domains of war' and 'multi-domain operation construct'. must be understood. Michael P. Kreuzer opines that layers of warfare constitute the mediums through which military activities may be orchestrated, while domains of warfare constitute sphere of operating environment that has physical characteristics and is guided by defined doctrines and organisational structures.

Cyber operations must be looked at, from a holistic viewpoint. Every domain of warfare, be it land, sea, air or space, is heavily dependent on cybertechnology and information technologies. In view of this, classifying cyberspace as a separate domain ignores the crucial role played by cyberspace in these domains. Therefore, Kreuzer argues that cyberspace must be classified as a

[1] Department of Defense Strategy for Operating in Cyberspace (2011). *Department of Defense (United States' Government)*. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

[2] Peixi, Zu (2021). A Chinese Perspective on the Future of Cyberspace. *Cyberstability Paper Series: New Conditions and Constellations in Cyber (pub. Global Commission on the Stability of Cyberspace & The Hague Centre for Strategic Studies)*. https://cyberstability.org/wp-content/uploads/2021/06/A-Chinese-Perspective-on-the-Future-of-Cyberspace-1-1.pdf

‘multi-domain operational construct’ as cyberspace involves the marriage of electronic and cyber layer of warfare with all physical domains of warfare.[3]

Integration of Cybertechnologies in the Traditional Domains of Warfare

In order to further understand the reason behind the classification of cyberspace as a multi-domain operational construct, the integration of cybertechnologies into the military operations in the traditional domains of warfare must be analysed. Countries have started purchasing military equipment and systems that are integrated with cybertechnologies. The United States Air Force (USAF) possesses the EC-130 Compass Cell electronic attack plane that could induce a combination of electronic and cyber-attacks on the opponent.[4] In May 2015, Israel signed an agreement to procure and deploy four “Sa’ar 6” ships to predominantly guard Israeli economic waters. Sa’ar 6 vessels are equipped with advanced electronic warfare and cyber defence capabilities that could be extensively used in surveillance and intelligence operations by the Israeli Navy.[5]

In 2021, the Israel Aerospace Industry (IAI) equipped the Sa’ar 6 vessels with far more offensive capabilities, including in the cyber sphere.[6] On the other hand, multiple reports suggest that the People’s Liberation Army (PLA) had deployed its AI and cyber-powered killer robots with

[3] Kreuzer, Michael P (2021). Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age. *The Strategy Bridge*. https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age

[4] Bommakanti, Kartik (2021). Cyber offence in the context of military operations. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/cyber-offence-in-the-context-of-military-operations/

[5] IDF (2018). Meet the new “Sa’ar 6” ships. *The Israel Defense Forces (IDF)*. https://www.idf.il/en/minisites/israeli-navy/meet-the-new-sa-ar-6-ships/

[6] Manaranche, Martin (2021). IAI Integrates Naval Combat Suite on Israeli Sa’ar 6 Corvettes. *Naval News*. https://www.navalnews.com/naval-news/2021/07/iai-integrates-naval-combat-suite-on-israeli-saar-6-corvettes/

offensive cyber and electronic capabilities near the Indian border during the longstanding standoff between India and China in 2021.[7]

In the domain of space, countries like the Islamic Republic of Iran and the Democratic People's Republic of Korea have continuously interfered with satellite communication through cyberattacks. Iran is accused of jamming the satellite communication of broadcasters such as the BBC from broadcasting Persian-language programmes in the country, along with interfering in the broadcasting of news channels during the 2012 Arab Spring and the 2009 Iranian Presidential elections, while North Korea is accused of interfering with the GPS-systems and satellite communications of South Korea; regularly disrupting aviation and other satellite communication-dependent sectors, between 2010 and 2012.[8]

With countries further looking to upgrade their weapon systems with advanced cyber capabilities, cyberspace and cyber-powered operations is being widely deployed in all traditional domains of warfare; making it a multi-domain operational construct, as construed by Kreuzer.

Offensive Cyber Capabilities and Defensive Cyber Capabilities

Countries are involved in types of cyberspace operations: cyber offensive operations and cyber defensive operations. Cyber offensive operations, or in other words, offensive cyber capabilities (OCC) is defined as "the combination of people, technologies and organizational attributes that jointly enable offensive cyber operations: the adversarial manipulation of digital services and

[7] Chinese PLA Deploys Machine Gun Wielding Robots Near Indian Border; Will Robotic Warriors Change The Battles of Future (2022). *The Eurasian Review*. https://eurasiantimes.com/chinese-pla-deploys-machine-gun-wielding-robots-near-indian-border-will-robotic-warriors-change-the-battles-of-future/

[8] Rajagopalan, Rajeshwari Pillai (2019). Electronic and Cyber Warfare in Outer Space. *The United Nations Institute for Disarmament Research (UNIDIR)*, Space Dossier 3. https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf

networks," by Egloff and Shires.[9] This definition has been chosen in view of the lack of a universally-agreed definition as states have conflicting definitions of 'offensive cyber capabilities'; the United States' doctrine defining OCCs to include cyberspace operations while the Australian Strategic Policy Institute (ASPI) including only the 'resources, information, skills and technical know-how' needed to orchestrate a cyberspace operation.[10]

Defensive Cyber Capabilities may include anti-access/information denial activities as well as eliminating situations conducive for cyber offensive operations, using the combination of people, technologies and organisational attributes. Or in other words, defensive cyber capabilities could be understood as the defence against the adversarial manipulation of digital services and networks that may arise due to cyber offensive operations and capabilities.[11]

Countries have been traditionally involved in enhancing their cyber defensive capabilities against belligerent hacking groups of non-state actors; however, in the twenty-first century with the overreliance on digital and cyber technologies, there has been wide claims of state-sponsored attacks on other states' critical infrastructure and servers through sophisticated cyberespionages and offensive operations with a destructive intention. There has been increasing overhaul in the race to achieve technological supremacy in the twenty-first century, with countries extensively researching and developing internet-of-things (IoT) and artificial intelligence technologies in order to integrate them with administrative and military operations.

Big Data Analytics (BDA) and Cloud Computing has gained prominence in recent years with research pointing out that data driven by cloud computing could help governments in decision-

[9] Egloff, Florian J & Shires, James (2021). Offensive Cyber Capabilities and State Violence: Three Logics of Integration. *Journal of Global Security Studies*, 7:1. https://doi.org/10.1093/jogss/ogab028

[10] Chawla, Gunjan & Srivastava, Vagisha (2020). What Are 'Offensive Cyber Capabilities'. *Medianama*. https://www.medianama.com/2020/08/223-what-are-offensive-cyber-capabilities/

[11] Fanelli, R (2016). Cyberspace Offense and Defense. *Journal of Information Warfare (pub. Peregrine Technical Solutions)*, 15:2, 53-65. https://www.jstor.org/stable/10.2307/26487531

making by aiding data analysis.[12] This warrants a natural overreliance on cyberspace and cybertechnologies. Overreliance on cyberspace and cybertechnologies automatically makes the state more susceptible to cyberattacks and offensive cyber operations.

Offensive Cyber Capabilities of States: Specific Focus on the U.S., China and Russia

States have started to believe in the theory of "the best defence is a good offence" that was formerly observed in the 'just war' theories and President Bush's pre-emptive action' doctrine after the 9/11 attacks.[13] States have increasingly invested in enhancing their cyber offensive capabilities to counter their adversaries.

The United States, the only tier 1 cyber power country according to the country-wise cyber power net assessment conducted by the International Institute of Strategic Studies,[14] has capacitated its national intelligence agency: the CIA, with advanced and sophisticated offensive cyber capabilities that are used for espionage and targeted attacks. The Chinese researchers very recently exposed CIA's and Northrop Grumman's joint-development: 'Beehive', a U.S. military malware that is used to monitor and attack international targets. Reports from Global Times, a state-run media house of the Communist Party of China, claim that Beehive is a platform that supports remote scanning, internet penetration, secret theft and even system destruction, and that the CIA deployed this malware in adversary states to recover key information as a part of CIA's

[12] Sazu, Mesbaul Haque & Jahan, Sakila Akter (2022). Impact of Big Data Analytics on Government Organizations. *Management & Data Science*, 6:2. https://doi.org/10.36863/mds.a.20157

[13] Zajac, Daniel L (2003). The Best Defense Is A Good Offense: Preemption, Ramifications For The Department of Defense. *USAWC Strategy Research Project (Pennsylvania: U.S. Army War College)*. https://apps.dtic.mil/sti/pdfs/ADA415796.pdf

[14] Cyber Capabilities and National Power: A Net Assessment (2021). *The International Institute for Strategic Studies (IISS)*. https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one

cyberespionage and intelligence operations, in an attempt to retain cyberspace hegemony.[15] Chinese researchers have also released information that exposes National Security Agency (NSA)-affiliated hacking groups in the U.S. to have hacked into critical servers of research institutes in countries like Russia, China, India and Japan. ‘Bvp47’ is an advanced attack tool developed by these hacking groups that facilitates a covert backdoor-like communication technology and secured sensitive and confidential information from critical servers. In India, servers of Indian Academy of Sciences in Bengaluru, Benaras University, and the Institute of Microbial Technology (IMTech) were tapped into, according to Chinese sources.[16]

It is also noted that the United States has incorporated cyberattacks as a part of their central strategy against Iran. Operation Olympic Games, launched during the Bush Tenure in 2006, featured a host of sophisticated targeted cyberattacks against Iranian nuclear facilities. President Obama is also believed to have continued with the cyberattack operation against Iran. The 2010 Stuxnet virus that severely affected the Natanz Nuclear Facility in Iran is an offensive cyber operation orchestrated by the United States as a part of the Operation Olympic Games. President Trump did nothing different by widening the scope of the CIA to launch cyberattacks against Iran.[17]

[15] Siwei, Zhao (2022). How CIA uses cyber weapon ‘Beehive’ to monitor, attack global key targets. *Global Times*. https://www.globaltimes.cn/page/202204/1259749.shtml

[16] Krishnan, Ananth (2022). U.S. group hacked top research institutes in India, Russia and China, says Beijing cyber firm. *The Hindu*. https://www.thehindu.com/news/international/us-group-hacked-top-research-institutes-in-india-russia-and-china-says-beijing-cyber-firm/article65079559.ece

[17] Hanna, Andrew (updated: 2021). The Invisible U.S.-Iran Cyber War. *The Iran Primer (United States Institute of Peace)*. https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war

China, on the other hand, has been accused of disrupting the Ladakh electricity grid in December 2021;[18] along with its involvement in the Mumbai Power Outage in 2020,[19] and the failure of the Northern electricity grids causing major power outages in North India, in 2012.[20] The Cybersecurity & Infrastructure Security Agency of the United States published their research in 2022 that alerted the international community about China's state-sponsored hackers exploiting the vulnerability of service providers and networks, called the Common Vulnerabilities and Exposures (CVEs).

It was also reported that Chinese state-sponsored hackers intrude into compromised servers, known as hop points, through Chinese Internet Service Providers (ISPs) by leasing remote access from the service providers. These state-sponsored hackers further identify critical Remote Authentication Dial-In User Service (RADIUS) and gain access through Structured Query Language (SQL) databases to gain access of passwords and sensitive information from users as well as government databases.[21] Post U.S. official Nancy Pelosi's visit to Taiwan, China has rampantly involved in cyberattacks and cyberespionages against the Taiwanese government to spy on Taiwanese interactions with the United States. The APT10 group backed by the Chinese Communist Party orchestrated several cyberattacks on Taiwanese government networks, websites, as well as in the public domain such as aviation, banking, satellite communication, industrial factory automation, consumer electronics, and so on, causing widespread economic

[18] Bommakanti, Kartik (2022). Chinese cyberattacks against Ladakh electricity grid: A déjà vu. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/chinese-cyberattacks-against-ladakh-electricity-grid/

[19] Cyber-attack from China behind Mumbai power outage in 2020 (updated: 2021). *Business Today.In*. https://www.businesstoday.in/latest/economy-politics/story/cyber-attack-from-china-behind-mumbai-power-outage-in-2020-289648-2021-03-01

[20] Anita (2012). China's hand in India's power blackout. *One India*. https://www.oneindia.com/2012/08/22/china-s-hand-in-india-s-power-blackout-1057676.html

[21] People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices (2022). *Cybersecurity & Infrastructure Agency (CISA)*. Alert (AA22-158A). https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

disarray.[22] China is also known to repeatedly involve in cyberattacks and cyberespionage operations against Southeast Asian nations as well as Japan, Australia and South Korea.

Russia is a state that has often resorted to cyber offensive operations against its adversaries such as Ukraine, the United States, and countries in the west predominantly through Distributed Denial-of-Service (DDoS) attacks and tapping into servers and critical infrastructure through malicious military malware. The Federal Security Service of the Russian government (erstwhile Federal Security Board (FSB)), along with state-sponsored hacking groups in Russia, have targeted the energy industry of European and North American countries along with their aviation industry and military operations. It was reported that in 2017, Russian Federal Security Service employees hacked into U.S. military and federal agency personnel's emails and messages, as well as journalists critical of the Kremlin as a part of their greater cyberespionage operation against the United States.[23]

Russia, along with Iran and China has actively tried to interfere in the U.S. Presidential Elections, both in 2016 and in 2020. Fancy Bear (also known as APT28) is a hacking group that is backed by the Russian military agency that involved in orchestrated sophisticated password phishing campaign against the Americans through spear phishing, a sophisticated hacking technique to obtain users' passwords and sensitive credentials. Fancy Bear is believed to have worked on turning the election tide in favour of President Trump, against the Democratic presidential candidate Hillary Clinton, in 2016.[24] Russia orchestrated several cyberattacks against Ukraine from December 2021 to March 2022, a few days from the beginning of the war in February.

[22] Sharma, Aakash (2022). Cyber attacks on Taiwan: China caught in its own tangle. *India Today*. https://www.indiatoday.in/world/story/cyber-attacks-on-taiwan-china-caught-in-its-own-tangle-1984633-2022-08-06

[23] Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (2022). *Cybersecurity & Infrastructure Agency (CISA)*, Alert (AA22-110A). https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[24] O'Niell, Patrick Howell (2020). The Russian hackers who interfered in 2016 were spotted targeting the 2020 US election. *MIT Technology Review*. https://www.technologyreview.com/2020/09/10/1008297/the-russian-hackers-who-interfered-in-2016-were-spotted-targeting-the-2020-us-election/

Microsoft reported that that Russian agencies and state-backed Russian hacking groups carried out around 110 cyberattacks on Ukraine between December 2021 and March 2022. Experts suggest that Russia hinted an invasion into Ukraine by initially orchestrating deadly cyberattacks and offensive cyber operations against Ukraine. On 23 February 2022, the eve of Russian invasion into Ukraine, Russian intelligence agency-affiliated hacking group, Iridium, released a destructive malware called FoxBlade on hundreds of Ukrainian military and government networks simultaneously.[25] It was further reported that Russia also uses cyberattacks as a substitute for war; Russia's hacking of the critical infrastructure of Estonian banks, parliament and government ministries in 2007 and the Russian cyberattacks on Finnish critical infrastructure in the aftermath of inviting the Ukrainian President Zelenskiy to speak in the Finnish Parliament in April 2022, putting case in point.[26]

Conclusion: What Trend Do the U.S., China and Russia Set to the International Community?

Increased cyber offensive capabilities and operations amongst prime adversaries such as the U.S., China and Russia have pushed the international community into a state of panic. States have realised the damage cyberattacks and offensive cyber operations may have on their economy and critical infrastructure and have resorted to strengthening their cyber offensive capabilities in line with the United States, China and Russia. India, for instance, is a tier 3 country in terms of cyber power and hasn't focused much on enhancing its cyber offensive capabilities until the 2000s. It has now outsourced its offensive cyberspace operations and

[25] Orenstein, Mitchell (2022). Russia's Use of Cyberattacks: Lessons from the Second Ukraine War. *Foreign Policy Research Institute (FPRI)*. https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

[26] Ibid

activities to private players such as SideWinder, which is an Indian national advanced persistent threat (APT) group that targets India's principal adversaries such as China and Pakistan.[27]

Similar to how adversaries of nuclear powers experience security dilemma to an enormous degree, adversaries of states with sophisticated cyber offensive capabilities have also started building on their offensive cyber capabilities. European nations have invested in researching and developing 'cyberweapons' to enhance their offensive cyber capabilities,[28] perhaps to reduce their reliance on the United States, that makes their adversaries in Asia in turn build their offensive cyber capabilities in accordance with the 'security dilemma' theory of realism.

Therefore, it is safe to conclude that the international community is headed towards working on their offensive cyber capabilities not just with an intention to involve in belligerent cyber activities but also as cyber defence to deter cyberattacks and offensive cyberoperations against them.

[27] Bhan, Aditya (2022). Will Private Actors Spearhead India's Offensive Cyber Capabilities to Counter China. *News 18*. https://www.news18.com/news/opinion/will-private-actors-spearhead-indias-offensive-cyber-capabilities-to-counter-china-4831835.html

[28] Europe Is Developing Offensive Cyber Capabilities. The United States Should Pay Attention (2017). *Council on Foreign Relations*. https://www.cfr.org/blog/europe-developing-offensive-cyber-capabilities-united-states-should-pay-attention

Bibliography

1. Department of Defense Strategy for Operating in Cyberspace (2011). *Department of Defense (United States' Government)*. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

2. Peixi, Zu (2021). A Chinese Perspective on the Future of Cyberspace. *Cyberstability Paper Series: New Conditions and Constellations in Cyber (pub. Global Commission on the Stability of Cyberspace & The Hague Centre for Strategic Studies)*. https://cyberstability.org/wp-content/uploads/2021/06/A-Chinese-Perspective-on-the-Future-of-Cyberspace-1-1.pdf

3. Kreuzer, Michael P (2021). Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age. *The Strategy Bridge*. https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age

4. Bommakanti, Kartik (2021). Cyber offence in the context of military operations. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/cyber-offence-in-the-context-of-military-operations/

5. IDF (2018). Meet the new "Sa'ar 6" ships. *The Israel Defense Forces (IDF)*. https://www.idf.il/en/minisites/israeli-navy/meet-the-new-sa-ar-6-ships/

6. Manaranche, Martin (2021). IAI Integrates Naval Combat Suite on Israeli Sa'ar 6 Corvettes. *Naval News*. https://www.navalnews.com/naval-news/2021/07/iai-integrates-naval-combat-suite-on-israeli-saar-6-corvettes/

7. Chinese PLA Deploys Machine Gun Wielding Robots Near Indian Border; Will Robotic Warriors Change The Battles of Future (2022). *The Eurasian Review*. https://eurasiantimes.com/chinese-pla-deploys-machine-gun-wielding-robots-near-indian-border-will-robotic-warriors-change-the-battles-of-future/

8. Rajagopalan, Rajeshwari Pillai (2019). Electronic and Cyber Warfare in Outer Space. *The United Nations Institute for Disarmament Research (UNIDIR)*, Space Dossier 3. https://unidir.org/sites/default/files/publication/pdfs//electronic-and-cyber-warfare-in-outer-space-en-784.pdf

9. Egloff, Florian J & Shires, James (2021). Offensive Cyber Capabilities and State Violence: Three Logics of Integration. *Journal of Global Security Studies*, 7:1. https://doi.org/10.1093/jogss/ogab028

10. Fanelli, R (2016). Cyberspace Offense and Defense. *Journal of Information Warfare (pub. Peregrine Technical Solutions)*, 15:2, 53-65. https://www.jstor.org/stable/10.2307/26487531

11. Sazu, Mesbaul Haque & Jahan, Sakila Akter (2022). Impact of Big Data Analytics on Government Organizations. *Management & Data Science*, 6:2. https://doi.org/10.36863/mds.a.20157

12. Zajac, Daniel L (2003). The Best Defense Is A Good Offense: Preemption, Ramifications For The Department of Defense. *USAWC Strategy Research Project (Pennsylvania: U.S. Army War College)*. https://apps.dtic.mil/sti/pdfs/ADA415796.pdf

13. Cyber Capabilities and National Power: A Net Assessment (2021). *The International Institute for Strategic Studies (IISS)*. https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one

14. Siwei, Zhao (2022). How CIA uses cyber weapon 'Beehive' to monitor, attack global key targets. *Global Times*. https://www.globaltimes.cn/page/202204/1259749.shtml

15. Chawla, Gunjan & Srivastava, Vagisha (2020). What Are 'Offensive Cyber Capabilities'. *Medianama*. https://www.medianama.com/2020/08/223-what-are-offensive-cyber-capabilities/

16. Krishnan, Ananth (2022). U.S. group hacked top research institutes in India, Russia and China, says Beijing cyber firm. *The Hindu*. https://www.thehindu.com/news/international/us-group-hacked-top-research-institutes-in-india-russia-and-china-says-beijing-cyber-firm/article65079559.ece

17. Hanna, Andrew (updated: 2021). The Invisible U.S.-Iran Cyber War. *The Iran Primer (United States Institute of Peace)*. https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war

18. Bommakanti, Kartik (2022). Chinese cyberattacks against Ladakh electricity grid: A déjà vu. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/chinese-cyberattacks-against-ladakh-electricity-grid/

19. Cyber-attack from China behind Mumbai power outage in 2020 (updated: 2021). *Business Today.In*. https://www.businesstoday.in/latest/economy-politics/story/cyber-attack-from-china-behind-mumbai-power-outage-in-2020-289648-2021-03-01

20. Anita (2012). China's hand in India's power blackout. *One India*. https://www.oneindia.com/2012/08/22/china-s-hand-in-india-s-power-blackout-1057676.html

21. People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices (2022). *Cybersecurity & Infrastructure Agency (CISA)*. Alert (AA22-158A). https://www.cisa.gov/uscert/ncas/alerts/aa22-158a

22. Sharma, Aakash (2022). Cyber attacks on Taiwan: China caught in its own tangle. *India Today*. https://www.indiatoday.in/world/story/cyber-attacks-on-taiwan-china-caught-in-its-own-tangle-1984633-2022-08-06

23. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (2022). *Cybersecurity & Infrastructure Agency (CISA)*, Alert (AA22-110A). https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

24. O'Niell, Patrick Howell (2020). The Russian hackers who interfered in 2016 were spotted targeting the 2020 US election. *MIT Technology Review*. https://www.technologyreview.com/2020/09/10/1008297/the-russian-hackers-who-interfered-in-2016-were-spotted-targeting-the-2020-us-election/

25. Orenstein, Mitchell (2022). Russia's Use of Cyberattacks: Lessons from the Second Ukraine War. *Foreign Policy Research Institute (FPRI)*. https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/

26. Bhan, Aditya (2022). Will Private Actors Spearhead India's Offensive Cyber Capabilities to Counter China. *News 18*. https://www.news18.com/news/opinion/will-private-actors-spearhead-indias-offensive-cyber-capabilities-to-counter-china-4831835.html

27. Europe Is Developing Offensive Cyber Capabilities. The United States Should Pay Attention (2017). *Council on Foreign Relations*. https://www.cfr.org/blog/europe-developing-offensive-cyber-capabilities-united-states-should-pay-attention