INTA 606 Final Paper

Non-proliferation of cyberwar and digital relations between nations

Non-proliferation of war reaches nearly every subdiscipline of modern warfare, including biological, chemical, and nuclear but fails to address the issue of cyberwarfare from the weapons control perspective. Multiple UN resolutions have tried to tackle the issue. Still, they cannot address it properly since they fail to look at the issue due to the nature of cyberweapons, their development, conservation, distribution, and usage, making it a complicated domain to regulate. Compared to space, where satellites can be tracked and observed, and their communications intercepted to understand their origin and functioning, cyberweapons are only understood once used and reverse-engineered. Cyber war is becoming more and more prevalent, with experts fearing a major disaster that could spark another world war. Unlike nuclear, cyber is a domain where dual-use technologies reign, with common consumer devices being used for acts that could be qualified as declarations of war. Active measure campaigns add a whole new level to the issue, as there was never a technical breach in the first place. The issue is therefore trying to incite countries not to commit cyber-attacks against one another, either directly as some units of the PLA have done in the past, or indirectly, using non-state actors. The UN's response to this kind of issue has always been to create a new agency or governing body but the cyber domain adds a new set of challenges to the issue of non-proliferation that other countries may try to exploit for nefarious means. It is therefore important to understand why countries would cooperate or refuse to do so when it comes to disclosing cyber capabilities or preventing attacks and how they can do this while maintaining sovereignty.

To avoid a cyber-apocalyptic scenario from happening, the UN has introduced a series of resolutions aimed at combating the criminal misuse of information technologies and protecting critical infrastructure. Resolutions have additionally started addressing nation-states' behaviors in cyberspace, with resolution 73/266 calling it an issue of "International security"[i] and resolution 73/27 establishing a working group on transparency and security on the use of information and communication technologies[ii]. While the idea of a working group that strives to develop rules and norms for cyberspace may be a good introduction to the problem, it fails to address many of the obstacles that it will face due to the nature of the problem. More recently, the UN introduced resolution 75/240[iii] to renew that open-ended working group (OEWG) until 2025 and has already produced a variety of documents, with the latest (as of April 2024) being a joint working paper between multiple member states. This paper calls for the exploration of capabilities needed to implement "Confidence Building Measures" between nations and recognizes the need for a state to have a "diplomatic service, cyber security strategy, and functioning [Cyber Emergency Response Team]" to be able to exchange information[iv].

While the previous working group seems to focus more on the issue of defensive security, it does not look into offensive capabilities or cyber espionage. The Tallinn manual explicitly states, in rule 32, that cyber espionage does not "violate international law"[v] but methods employed may not be a practice of good faith, especially if this intelligence disrupts a "peaceful settlement of disputes" and prevents a State from presenting a case[vi].

For countries to be able to cooperate and exchange about cyber-related issues, especially offensive ones, there needs to be a way to disclose such capabilities while ensuring the protection of methods and techniques. A solution could therefore be to create a UN agency, similar to the IAEA to deal with the issue, perform inspections, and ensure a certain cyber nonproliferation. Since a black marker does not work for software, there must be a new way for nation-states to expose their capabilities and allow experts to evaluate the true capabilities of a weapon, all without revealing the source code itself or allowing counter-weapons to be created. The issue here lies in the dual use of information technology and the inability of one to detect its true nature without having access to the system. In a 2020 article[vii], the National Defense University argues that cyberweapons, when looking at their classification for policy-making purposes, can be compared to kinetic weapons by their effect, associated policies, and targeting practices. While kinetic weapons are aimed at a single target and engineered to strike all, or at least a certain variety of targets, cyberweapons can adapt to a multitude of systems and re-engineered on the go, sometimes reprogramming themselves to better take down the very system at which they are aimed. Cyberweapons are quite simple to use and can be put in the hands of almost anyone who knows how to operate a computer while kinetic weapons will require training, sometimes extensive, to use. Effect and impact are also contrasting attributes between cyber and kinetic weapons. Kinetic weapons are scalable by volume and have a predictable and immediate effect and effectiveness while cyber weapons are scalable with their use and susceptible to changes. Obsolescence is a common point between both weapon types and one often not discussed. As cyberweapons rely on a vulnerability to effectively deliver their payload, the lifetime of such offensive software relies entirely on whether that vulnerability has been patched, as noted by Capt. Bartos of the US Naval Institute[viii]. Evaluating a cyberweapon's effect and estimating its shelf life are therefore key factors in the classification of its potential dangerousness.

Bioweapons bring a new aspect of the question into play, that of dual-use technologies. As UN resolution 73/27 points out, "[Information and Communication Technologies] are dual-use technologies and can be used for both legitimate and malicious purposes"[ix]. Bioweapons and laboratories associated have long been branded as legitimate concerns but serve a dual-purpose role, both in the study of what other nations might be working on and the development of vaccines. This can be said for the Wuhan Institute of Virology, where scientists are working on coronaviruses, or Fort Detrick which houses the US military's biomedical research facilities. Just like legitimate tools studied in laboratory conditions can be studied on subjects and then accidentally escape the facility, cyberweapons can have the same unintended effect. The Snowden leaks, not just the documents but the tools used by the NSA, have set American cyber capabilities back years and enabled other nations to conduct their operations[x]. The comparison can therefore be made between the modification of bioweapons for increased lethality or targeted effect, while cyberweapons can be reengineered for effectiveness or systems targeting. Similarly, both biological and cyber weapons are modified to increase contamination. Evaluation, classification, and disclosure become important to understand the rate at which a cyberweapon can make its way from one system to another, like a virus' contamination rate. The parallel has already been made by researchers in cybersecurity and virology alike, leading to an adaptation of "techniques of mathematical epidemiology" to study computer virus propagation[xi].

Just as the UNGA is trying to reduce the misuse of Information and Communication Technologies (ICTs)[xii], the WHO has had similar initiatives for bioweapons like the Biosafety Manual[xiii] but can only give recommendations. The US government had also included the screening of certain gene sequence orders or chemicals that may be used to create weapons of mass destruction, which had succeeded in the past when a Saudi student tried to "construct an IED using several chemicals"[xiv].This however fails to address commercially available products, just like certain pen-testing software suites can be used for nefarious means. A major advantage of dual-use software and widely available pen testing tools is that their behavior is already well-known, and systems can very easily detect their use.

Nuclear weapons and their restrictions have also been at the heart of countless US resolutions[xv] and international initiatives. This is due to their potentially devastating effects, both in the short term with the shock wave and the long-term radiation and fallout. The International Atomic Energy Agency (IAEA) and its visits to nuclear sites around the world are the nuclear solutions to trying to enforce non-proliferation and prevent Chernobyl-like disasters from happening again. The IAEA oversees collecting states' reports and declarations of nuclear activities while ensuring sites cannot house illegal enrichment centrifuges during their construction and can perform routine inspections[xvi]. Cyberwarfare is completely different in the sense that an attack does not require a large facility, needing a small server room at best. However, the outsourcing of attacks (and thus of associated hardware), might prevent such inspections from taking place. Additionally, simply looking at a server room does not tell you much about what it does and what might be running on it. Inspectors might be fooled if someone logs into a server by allocating different permissions to the account presented as opposed to the administrative account. This leads to the question of being able to effectively check what a country is developing for cyber offense without looking directly at the source code. The issue when comparing to other domains of warfare and how international law applies to weapons development is that for each case, nation-states have found a way to hide their weapons from inspections and the international community. Cyber weapons follow a similar trend. Some nations proudly display their cyber units like Israel's unit 8200[xvii], which sees its veterans get highly paid jobs in the tech industry, while others like the United States adopt a posture of "deterrence by denial"[xviii]. Admitting to conducting offensive cyber operations, as a major player on the world stage, would only enable others to believe that it is a viable and authorized method of conducting a deniable war.

Just like nations publicly disclosed their number of COVID cases during the pandemic to inform travelers and help other countries with their foreign policy, the same should be applied to cyberweapons to help other nations adjust their policies when one is accidentally released from a lab. According to the Department of Justice, an overwhelming number of cyber-attacks go unreported[xix], likely for companies to maintain their stock values. Because of this, many people's confidential information is either released into forums or sold to the highest bidder (who will likely use it for nefarious purposes.) Disclosures of weapons used and their circulation on the market is one aspect of this issue, another one is disclosing the vulnerabilities in your systems. Many companies have instituted bug-bounty programs, in which private actors can voluntarily report the vulnerabilities that they have found in a system in exchange for compensation. For example, Microsoft will offer up to $20,000 for a vulnerability found in the Xbox Live network[xx]. Compared to having an in-house cybersecurity team, this solution is much cheaper and allows for a more ethical, community-based solution rather than having to fix problems after they have been discovered. Certain people, however, thrive off exploits for unethical reasons, selling them on specialized sites like BreachForums, for profit[xxi]. This raises a few more questions of ethics because employees of firms may be tempted to deliberately leave vulnerabilities in their systems to then sell them to the highest bidder instead of patching them. The cyber world also sees its fair load of weapons trafficking which may entice employees of firms or government agencies to deliberately steal the very programs they have been working on for years and sell them to the highest bidder. An often-undiscussed fact of the Snowden case is the theft of multiple tools the NSA had been working on for years and according to the Intercept, ended up on the black market[xxii]. Experts including David Sanger[xxiii] compare this to the beginning of the new cyber–Cold War and arms race, like the nuclear race of the last century.

Disclosing cyber capabilities can easily be done without revealing source code by sandboxing a weapon, showing its capability in a closed environment, and allowing for evaluation. Sandboxing is commonly used in cybersecurity defensive operations to evaluate a malware's behavior without compromising a machine and tracking interactions with the network, file system, and function calls. Getting such information could help understand how the weapon contaminates other machines and communication patterns, allowing for its detection in the event of an attack on a hospital or another critical infrastructure. Sandboxing does have its limits, mainly in the handling of zero-day exploits, false positives and negatives as well as known sandboxing evasion techniques[xxiv]. Aviation has airshows to demonstrate the maneuvering abilities of an aircraft and we are still very far from seeing public displays by militaries of cyber capabilities.

The idea of having a governing body to monitor and regulate cyber weapons may seem like a great idea but comes with numerous challenges, both technical as outlined above, and political. The United States openly denies all its cyber offensive operations, even at times when it might be behind them as illustrated towards the beginning of the war in Ukraine[xxv]. Admitting to a cyber-attack would of course encourage other nations to engage in similar behavior, especially on more critical infrastructure as opposed to military targets. Disclosure of such attacks would also give the attacked nation a valid reason to strike back, just like an admission of kinetic attacks has justified retaliation by nation-states. A good recent example of such a phenomenon is the events in the Middle East, with Israel admitting to attacking the Iranian Consulate in Damascus and giving Iran a valid reason to retaliate[xxvi]. Going off realist theory, having that first-strike capability and being able to guarantee nations need to maintain the weight behind negotiations. Not being able to deliver a massive, yet plausibly deniable blow to another nation's critical military systems because of an international governing body is something many countries, including the United States and Russia, would oppose and veto at the UN. Russia is especially known for its inverse-militarized diplomacy strategy, which realists argue is the best way to approach the issue and has completely changed the way negotiations will be conducted. Cyber inverse-diplomacy fails at fitting into standard military negotiations since leaders display their capabilities to deter adversaries while cyber weapons lose "operational effectiveness when they cease to be secret" or can be attributed to a certain party[xxvii].

As more of a constructivist argument for the idea of using cyber weapons and their disclosure, some optimists have noted that cyber conflict cannot be escalatory "when states have never responded to cyber-attacks with traditional violence"[xxviii]. The issue therefore doesn't come from nation-states having cyber capabilities, like nuclear or kinetic weaponry, but from the fact a few nations have used them recklessly in the past or third parties can very easily acquire them. To prevent a worldwide cyber apocalypse from happening, as many experts are predicting for our near future, we therefore must come up with a set of regulative norms for states to follow to ensure the survival and good use of cyberspace by every actor that uses it. For this to happen though, most states would have to adopt it and internalize it in their practices. This would directly go against the realist argument and inverse-military diplomacy as some nations have done in the past.

Artificial intelligence and its rise has been in the minds of many recently, especially governments and cyber security researchers alike, who fear that an advanced enough polymorphic malware could infect "various systems and organizations to evade defense systems or even detection"[xxix]. In the event of a new polymorphic malware, especially one that is AI-enabled, there is a chance that it might go rogue and try to take over the world. Luckily, Mission Impossible authors have already taken hold of this scenario, as did many other science fiction writers before them but the latest movie (Dead Reckoning part two having not been released yet when writing this) perfectly illustrates how nations would react to such an event. In the movie, Ethan Hunt (Tom Cruise) must get control of a two-part key that will unlock the source code of an AI weapon designed for intelligence gathering but the system ends up going rogue[xxx]. Rather than come together to face a worldwide threat, every nation either sends its security service or hires proxies to try to get control of the entity to further weaponize it for its gain. While this is a Hollywood movie and many events are exaggerated, it does mirror similar reactions nations had during the COVID-19 pandemic, where states engaged in near adversarial behavior to ensure survival. Rumors, which ended up being confirmed, of Americans buying up masks "for three to four times their price" coming into France surfaced, and flourished all over European social media, causing a scandal[xxxi]. Security cooperation works with nations aligning against each other or coming together against a common enemy as much of the world did against Saddam Hussein during Operation Desert Storm but could see a shift in priorities and even betrayals if such a scenario were to take place. Nations would even go as far as to deny involvement, just like China did for the coronavirus pandemic, claiming the origins of Covid-19 "should not be politicized"[xxxii].

Looking at the Tallinn Manual can help understand nations' behavior in cyberspace, or at least what the international community should be doing, and can help establish an international framework and norms for nations to abide by when conducting offensive cyber operations. NATO's main rule book and "objective restatement of international law" [xxxiii] for cyber operations and conflicts, especially rules that pertain to civilians, private infrastructure, and cyber espionage would be contested by non-NATO member states, Russia especially, if used in the UN as a basis for international cyber non-proliferation and de-escalation. A lot of very good points, relevant to kinetic armed conflicts or revolutions are made, especially rule 37. This rule states that civilians who engage in cyber operations as part of a “Levée en masse” (mass rising) benefit from the same privileges as prisoners of war and armed combatants in a conflict, like that of a conventional army.[xxxiv] Further detail is added to Rule 32’s prohibition against the civilian population with the mention that only “cyberinfrastructure [...] if they are military objectives” may be targeted and attacks “without distinction” are prohibited.[xxxv] While a proper governing body may enforce these rules with nations, proxy groups, and other third parties would not fall under these restrictions, allowing countries to take advantage for their gain.

Russia has already proven to be using this strategy in the past, especially when in 2021, members of the REvil ransomware group were arrested for attacking the Colonial pipeline. REvil had since then benefitted from protection from the Russian government, so long as they don’t attack Russian computers and citizens, something they achieved by including a bit of code in their malware that would “avoid computers that use Russian”[xxxvi]. Ransomware gangs can avoid hospitals and other civilian critical infrastructure in the nations that host them through other methods like checking the public IP address against their region since they are geographically allocated. Russia has no extradition treaty with the United States, allowing cyber gangs to operate with total impunity but also giving Russia a new card to play during negotiations. As the healthcare sector often pays ransoms the quickest due to the urgency of needing to maintain operations, and American healthcare being at the forefront of technology, cyber gangs have made it their primary target. Other nations like North Korea have understood and adapted their cyber strategy accordingly to include the use of non-state actors. The Lazarus group usually operates overseas to maintain that degree of separation from the Hermit Kingdom while still affiliated with the North Korean military, especially for funding, recruitment, and other material support. Unlike

Russian cyber gangs who mainly target American and other Western businesses for money, North Korean groups do it for both political ideology and money, needing to bring in foreign funds to be able to acquire material for the illegal nuclear program their nation is running. A good example of an ideologically motivated attack was when wipeware was deployed to Sony Pictures Entertainment's systems as retaliation for Seth Rogen making a movie mocking North Korea, and more specifically their leader, Kim Jong Un. By keeping these groups at arm's reach but not fully incorporating them into their armed forces, nations like Russia and North Korea can maintain their plausible deniability all while having cyber capabilities. Both cases go to show that although an international governing body may be able to help combat such criminal activity, some nations will not cooperate since that activity directly benefits them.

Overall, a new governing body, focused on reducing cyber warfare and trying to create international cooperation between nations around this issue would struggle immensely due to the nature of the problem and certain nations' behaviors. The United States would have its reservations due to always denying their involvement in cyber offensive operations and maintaining its strategy of "deterrence by denial"[xxxvii] and others like Russia and North Korea would still engage in proxy operations using cyber gangs and kite groups. Nation states, if faced with the possibility of gaining an immense source of power and influence (the Entity), would turn on each other on that occasion, making security cooperation nearly impossible. Biological and nuclear weapons studies have a lot to teach us concerning nonproliferation and international cooperation in the face of cyber-realism and the race to a better weapon. While nations do have advantages in cooperating, mainly in protecting each other's critical civilian infrastructure, cyber realism dominates their decision-making and the potential for cooperation.

[i] United Nations, "UNGA Resolution 73/266 Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (General Assembly, January 2, 2019), https://documents.un.org/doc/undoc/gen/n18/465/01/pdf/n1846501.pdf.

[ii] United Nations, "UNGA Resolution 73/27 Developments in the Field of Information and Telecommunications in the Context of International Security," December 5, 2018, https://documents.un.org/doc/undoc/gen/n18/418/04/pdf/n1841804.pdf.
[iii] United Nations General Assembly, "UNGA Resolution 75/240: Developments in the Field of Information and Telecommunications in the Context of International Security," January 4, 2021, https://documents.un.org/doc/undoc/gen/n21/000/25/pdf/n2100025.pdf?token=QAcfAEmohSkYQiRqQD&fe=true.
[iv] UNGA OEWG, "Joint Working Paper Building Confidence and Capacity in a Cyber Way" (United Nations, April 23, 2024), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Joint_Working_Paper_CBMs_&_Capacity_Building.pdf.
[v] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017), https://doi.org/10.1017/9781316822524.
[vi] UNIDIR (United Nations Institute for Disarmament Research), "International Law and the Behaviour of States in the Use of ICT – Challenges and Opportunities" (United Nations, November 15, 2023), https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNIDIR_International_Law_and_the_Behaviour_of_States_in_the_Use_of_ICT.pdf.
[vii] Josiah Dykstra, Chris Inglis, and Thomas Walcott, "Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat," *Joint Force Quarterly* 99 (November 19, 2020), https://ndupress.ndu.edu/Media/News/News-Article-View/article/2421554/differentiating-kinetic-and-cyber-weapons-to-improve-integrated-combat/.
[viii] Capt. Christopher A. Bartos, USMC, "Cyber Weapons Are Not Created Equal," *US Naval Institute*, June 2016, https://www.usni.org/magazines/proceedings/2016/june/cyber-weapons-are-not-created-equal.
[ix] United Nations, "UNGA Resolution 73/27 Developments in the Field of Information and Telecommunications in the Context of International Security."
[x] Sam Biddle, "THE NSA LEAK IS REAL, SNOWDEN DOCUMENTS CONFIRM," *Theintercept.Com*, August 19, 2016, https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/.
[xi] Jeffrey O. Kephart and Steve R. White, "DIRECTED-GRAPH EPIDEMIOLOGICAL MODELS OF COMPUTER VIRUSES," in *Computation: The Micro and the Macro View*, by B A Huberman (WORLD SCIENTIFIC, 1992), 71–102, https://doi.org/10.1142/9789812812438_0004.
[xii] United Nations, "UNGA Resolution 73/27 Developments in the Field of Information and Telecommunications in the Context of International Security."
[xiii] World Health Organization, *Laboratory Biosafety Manual*, Fourth edition (Geneva: World Health Organization, 2020).
[xiv] US Department of Justice, "Saudi Student Sentenced to Life in Prison for Attempted Use of Weapon of Mass Destruction," November 13, 2012, https://www.justice.gov/opa/pr/saudi-student-sentenced-life-prison-attempted-use-weapon-mass-destruction.
[xv] United Nations General Assembly, "UNGA Resolution 71/258 Taking Forward Multilateral Nuclear Disarmament Negotiations" (United Nations, January 11, 2017), https://documents.un.org/doc/undoc/gen/n16/466/69/pdf/n1646669.pdf.
[xvi] United Nations, "About the IAEA," n.d., https://www.iaea.org/about/about-iaea.
[xvii] Israeli Ministry of Defence, "Military Intelligence Directorate of the IDF," December 29, 2021, https://www.idf.il/en/mini-sites/directorates/military-intelligence-directorate/military-intelligence-directorate/.
[xviii] LCDR Stephanie Pendino, MAJ Robert K. Jahn, and Kirk Pedersen, "U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light," *Joint Forces Staff College*, September 7, 2022, https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/.
[xix] US Department of Justice, "Report of the Attorney General's Cyber Digital Task Force," July 2, 2018, https://www.justice.gov/archives/ag/page/file/1076696/download.
[xx] Microsoft Corporation, "Microsoft Bug Bounty Program," n.d., https://www.microsoft.com/en-us/msrc/bounty.
[xxi] Sead Fadilpašić, "BreachForums Hacking Forum Admin Sentenced to 20 Years Supervised Release," January 22, 2024, https://www.techradar.com/pro/security/breachforums-hacking-forum-admin-sentenced-to-20-years-supervised-release.
[xxii] Biddle, "THE NSA LEAK IS REAL, SNOWDEN DOCUMENTS CONFIRM."
[xxiii] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, First paperback edition (New York: Broadway Books, 2019).
[xxiv] Bart Lenaerts-Bergmans, "WHAT IS CYBERSECURITY SANDBOXING?," *Crowstrike* (blog), September 12, 2023, https://www.crowdstrike.com/cybersecurity-101/secops/cybersecurity-sandboxing/.
[xxv] SC Staff, "US Denies Alleged Massive Cyberattack against Russia," *SC Media*, March 30, 2022, https://www.scmagazine.com/brief/us-denies-alleged-massive-cyberattack-against-russia.

[xxvi] Helen Regan, Hamdi Alkhshali, and Tamara Qiblawi, “Iran Vows Revenge as It Accuses Israel of Deadly Airstrike on Syria Consulate in Deepening Middle East Crisis,” *CNN*, April 2, 2024, https://www.cnn.com/2024/04/02/middleeast/iran-response-israel-damascus-consulate-attack-intl-hnk/index.html.

[xxvii] Richard Andres, “Inverted-Militarized Cyber Diplomacy,” *Georgetown Journal of International Affairs*, January 2014, 119–29.

[xxviii] Jason Healey and Robert Jervis, “The Escalation Inversion and Other Oddities of Situational Cyber Stability (Fall 2020),” 2020, https://doi.org/10.26153/TSW/10962.

[xxix] Bernard Marr, “Cyber Apocalypse 2023: Is The World Heading For A ‘Catastrophic’ Event?,” *Forbes*, February 6, 2023, https://www.forbes.com/sites/bernardmarr/2023/02/06/cyber-apocalypse-2023-is-the-world-heading-for-a-catastrophic-event/?sh=6ffa20391b70.

[xxx] Villains Wiki, “The Entity,” 2023, https://villains.fandom.com/wiki/The_Entity_(Mission:_Impossible).

[xxxi] France 24, “Coronavirus : Des Masques Commandés Par La France Rachetés ‘Sur Le Tarmac’ Par Les Américains,” April 2, 2020, https://www.france24.com/fr/20200402-coronavirus-des-masques-command%C3%A9s-par-la-france-rachet%C3%A9s-sur-le-tarmac-par-les-am%C3%A9ricains.

[xxxii] Economic Times, “China Rejects US Report’s Lab-Leak Theory on COVID-19 Origin,” *India Times*, February 27, 2023, https://economictimes.indiatimes.com/news/international/world-news/china-rejects-us-reports-lab-leak-theory-on-covid-19-origin/articleshow/98281233.cms?from=mdr.

[xxxiii] CCDCOE, “The Tallinn Manual,” *NATO Cooperative Cyber Defence Centre of Excellence*, n.d., https://ccdcoe.org/research/tallinn-manual/.

[xxxiv] Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

[xxxv] Schmitt.

[xxxvi] Malwarebytes Labs, “Ransomware’s Russia Problem,” *Malwarebytes* (blog), July 15, 2021, https://www.malwarebytes.com/blog/news/2021/07/ransomwares-russia-problem.

[xxxvii] LCDR Stephanie Pendino, MAJ Robert K. Jahn, and Kirk Pedersen, “U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light.”