

## Cyberattacks and the Use of Force

Graham Overcash

The twenty-first century has increasingly seen states have engaged in “gray zone” or “hybrid” warfare. Gray zone warfare can be defined as “competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality.”<sup>1</sup> Gray zone warfare renders “the line between war and peace” obsolete, making it hard to identify “the war threshold.”<sup>2</sup> Hybrid warfare has no clear definition, but is often “characterized by ambiguity about the nature of the conflict [and] opacity of the parties involved.”<sup>3</sup> One of the key tools in hybrid warfare is the use of cyberattacks. These attacks allow an actor to cause damage and disruption to a state but are less attributable and less escalatory than traditional kinetic means of attack such as bombs and missiles. For example, in 2010, the United States and Israel executed a cyberattack on Iran’s nuclear program that damaged nearly 1,000 of Iran’s nuclear centrifuges.<sup>4</sup> This attack caused physical damage to the Iranian nuclear program, however, Iran did not respond like they presumably would have for a traditional kinetic attack. Had an American aircraft bombed an Iranian nuclear facility and caused damage, Iran would have almost certainly responded in some significant way. Iran, however, does not seem to have responded in any significant way to America’s cyberattack. This leads to an observation that states are less likely to consider a cyberattack as serious as a state considers the use of force. This blog will examine when a country sees a cyberattack as constituting a use of force.

Article 2 of the United Nations (UN) charter states that “[a]ll Members shall refrain in their international relations from the threat or use.”<sup>5</sup> This prohibition on the use of force has become a foundational principle of the post-World War II international order. While the prohibition generally refers to “armed force,” the International Court of Justice has issued an advisory opinion that applies this prohibition “to any use of force, regardless of the weapons employed.”<sup>6</sup> This advisory opinion how some countries may see cyberattacks as a use of force.

Many states adopted the approach that “a cyber operation will constitute a use of force where its ‘scale and effects’ are comparable to a use of force by traditional kinetic means.”<sup>7</sup> “For

---

<sup>1</sup> United States Special Operations Command, *White Paper: The Gray Zone 1* (Sept. 9, 2015).

<sup>2</sup> Arsalan Bilal, *Hybrid Warfare: New Threats, Complexity, and Trust as the Antidote*, NATO Rev. (Nov. 30, 2021), <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.

<sup>3</sup> United States Special Operations Command, *supra* note 1.

<sup>4</sup> Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (June 1, 2012), [https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U\\_story.html](https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U_story.html).

<sup>5</sup> U.N. Charter art. 2, ¶ 4.

<sup>6</sup> *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 1996 I.C.J. 226 (July 8), at 22.

<sup>7</sup> *Cyber Affairs and Critical Technology*, Austl. Dep’t of Foreign Affs. & Trade, <https://www.dfat.gov.au/international-relations/themes/cyber-affairs-and-critical-technology> (last visited Oct. 24,

example, a cyber operation that destroys, inflicts damage, or permanently disables critical infrastructure or civilian objects within a State, may be considered as amounting to a use of force under international law.”<sup>8</sup> States are very protective of their “critical infrastructure” and are more likely to consider a cyberattack that targets critical infrastructure a use of force as opposed to an attack that targets less important systems.

While every state has their own definition of critical infrastructure, comparing America’s to Australia’s will reveal some common characteristics. Generally, infrastructure is critical when “its disruption or destruction would have a detrimental impact” on services that promote the social or economic stability of the state or its national security.<sup>9</sup> America defines critical infrastructure as “systems and assets, whether physical or virtual, so vital to the US that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters.”<sup>10</sup> However, Australia defines it as “physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security.”<sup>11</sup> Both states see critical infrastructure as including physical and digital systems and both states are concerned with systems that support national security. Furthermore, both states are keenly concerned with ensuring economic security and stability and view any system that supports those interests as critical. President Joe Biden warned Russia that attacks against critical infrastructure are “off-limits” and provided a list of sixteen sectors that America considers to be critical infrastructure.<sup>12</sup> This demonstrates how serious threats to a state’s critical infrastructure are. An attack on critical infrastructure could seriously impede a state’s ability to govern. The failure of critical infrastructure could be a potential existential threat to a state. For this reason, many states would consider a cyberattack on critical infrastructure as a use of force, which is evident in the African Union’s common positions.<sup>13</sup>

Not all states share this opinion, however. For instance, New Zealand’s position is that “a cyber operation causing significant loss of functionality to its [critical infrastructure] would

---

2024); *Letter from the Gov’t of the Kingdom of the Neth., Minister of Foreign Affs. to Parl.* at 3–4 (July 2019), <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/appendix-International-law-in-cyberspace-kingdom-of-the-netherlands.pdf>.

<sup>8</sup> Mohamed Helal, *Common Afr. Position on the Application of Int’l Law to the Use of Info. & Comm’n Techs. in Cyberspace*, Ohio State Legal Studies Research Paper No. 823, at 6-7 (Feb. 2, 2024).

<sup>9</sup> Samuli Haataja, *Cyber Operations Against Critical Infrastructure Under Norms of Responsible State Behaviour and International Law*, 30 Int’l J.L. & Info. Tech. 423, 427 (2022).

<sup>10</sup> USA Patriot Act of 2001, 42 U.S.C. §§ 5195c(e), 1016(e) (2018).

<sup>11</sup> Austl. Dep’t of Home Affs., *Critical Infrastructure Resilience Strategy 4* (2023).

<sup>12</sup> Vladimir Soldatkin & Humeyra Pamuk, *Biden Tells Putin Certain Cyberattacks Should Be “Off-Limits,”* REUTERS (June 16, 2021), <https://www.reuters.com/technology/biden-tells-putin-certain-cyber-attacks-should-be-off-limits-2021-06-16/>.

<sup>13</sup> Helal, *supra* note 8.

constitute a violation of the non-intervention principle, as opposed to the use of force.”<sup>14</sup> A violation of the non-intervention principle is less serious than a use of force, so it would be met with a less significant response.<sup>15</sup> Even though a cyberattack causing significant loss of functionality in a critical infrastructure system would be a serious threat to New Zealand, the government is unwilling to classify it as the use of force. For instance, if a state launched a missile at a power plant in New Zealand, resulting in blackouts, the government of New Zealand would almost certainly classify that as a use of force. Their government however, according to this policy, would likely not consider a cyberattack targeting their power grid that also resulted in blackouts as a use of force. This demonstrates how some states are less likely to label a cyberattack as the use of force, compared to a kinetic attack, even if the state would be greatly harmed by the cyberattack.

There is more ambiguity when the cyberattack only results in a loss of functionality of systems without causing physical damage.<sup>16</sup> An example is the Netherlands, which is the only country that “has suggested that a cyber operation could constitute a use of force where it had ‘a very serious financial or economic impact.’”<sup>17</sup> Under the view taken by the Dutch, a ransomware attack that asked for a large ransom could be seen as a use of force. This demonstrates a sharp contrast to New Zealand and the positions offered by other states. While states generally only see cyberattacks as constituting the use of force if there is physical damage or critical infrastructure is threatened, the Netherlands has applied a broader understanding of the use of force. This viewpoint offers an alternative understanding of cyberattacks and the use of force that could help develop a strong deterrent to cyberattacks such as ransomware.

As states are using gray zone warfare and cyberattacks to advance their interests, it is important to understand what constitutes breaches of international law and norms. Cyberattacks that cause physical damage or threaten critical infrastructures can be seen as a use of force. Individual states, however, have different understandings. Some states like New Zealand are less likely to call a cyberattack a violation of the prohibition on the use of force. While the Netherlands apply a broader understanding of what the use of force is in regards to cyberattacks. An international framework that could standardize when a cyberattack constitutes the use of force could lower the risk of unintended escalation and ensure a safer, more stable world.

---

<sup>14</sup> Haataja, *supra* note 11 at 434.

<sup>15</sup> *Id.*

<sup>16</sup> SAMULI HAATAJA, *CYBERATTACKS AND INTERNATIONAL LAW ON THE USE OF FORCE: THE TURN TO INFORMATION ETHICS* 89–95 (Routledge ed. 2019).

<sup>17</sup> Haataja, *supra* note 11 at 434.