Should nation states retaliate against intelligence operations carried out in cyberspace?

A legal and strategic analysis based on the case studies of Operation Aurora and Stuxnet

1. Cyber intelligence operations and their strategic role.

Cyber intelligence (CYBINT) operations are an increasingly common practice among nation-states. These operations are more commonly tied to state actors, referring to state-led or state-sponsored actions that use cyberspace to collect, analyze, and exploit foreign confidential information for national security purposes or economic statecraft, or at least justified as such (Cormac & Aldrich, 2018). This paper focuses only on operations conducted by or on behalf of a state for economic intelligence and/or national security purposes. Rogue cybercriminals, not tied to a state, aiming to simply blackmail or steal a victim's money are not considered to be CYBINT operations, and therefore are not the focus of this analysis.

The importance of CYBINT lies in the same principle as traditional intelligence: information is power. Whether it is information on adversaries, allies, or technology, the state with the best intelligence will always hold the upper hand in the international arena (Nye Jr, 2010). CYBINT is becoming the best method to gather intelligence on foreign companies or states, making it a top priority for nations, who spend significant resources on better developing their CYBINT capabilities and their cybersecurity structure. An efficient CYBINT operation can give a state insight into an adversary's plans, weaknesses, and technologies before a conflict even starts, which is precisely why cyber operations are carried out as much in peacetime as they are in wartime (Rid, 2013). Adversaries (and allies) are constantly gathering information on each other, keeping it a non-stop habit that keeps nations (especially global powers) in check.

Greenberg (2019) points out that one of the main reasons CYBINT continues to grow is because cyberspace itself keeps expanding. As technology advances, processes become automated, data moves to the cloud, and home networks increasingly overlap with corporate systems through remote work. Today, almost no machine or piece of information is completely disconnected from the internet[1]. Although this digitalization came with many advantages; greater storage capacity,

[1] Agencies like the CIA, NSA, Mossad, GCHQ, and others use air-gapped networks for their most classified systems. An air gap means the computer or network is physically isolated from the public internet or any unsecured system. These are used to store or process Top Secret / Sensitive Compartmented Information (TS/SCI) so it cannot be remotely accessed.

easier access, and faster information flows, it also introduced a major threat: the attack surface for both private companies and public institutions has become increasingly vast and vulnerable, and therefore a main subject of interest for adversaries to conduct cyber espionage and intelligence gathering. As a result, most of today's cyber operations are no longer focused on military targets but on economic intelligence; stealing private-sector secrets related to technological development to strengthen a state's economic position against its rivals (Cormac & Aldrich, 2018).

Whether it's a case of mere economic espionage or a sabotage operation meant to cripple an adversary's defense resources, CYBINT has become a pivotal tool in a state's national security strategy and economic statecraft. Therefore, as with traditional espionage and foreign intelligence missions, a state has the right to defend itself against CYBINT, and, under certain circumstances consistent with international law explained in this paper, it can also retaliate when it becomes the victim of a cyberattack or hostile cyber operation (Corn & Taylor, 2017).

2. Legal frameworks and thresholds for retaliation.

To address whether states may lawfully retaliate against cyber intelligence operations, it is necessary to examine the existing international legal framework, even if it remains unsettled. Using the *Tallinn Manual 2.0* and the precedents established by the case studies discussed in this paper, the thresholds and legal limits of retaliation become clearer. Once those boundaries are defined, the question shifts from what states may do under international law to what they *should* do as a matter of strategy and policy. For the purpose of defining the legal boundaries, this paper describes the main aspects to consider[2]:

1. *Sovereignty:* Sovereignty is the starting point for assessing the legality of a cyber operation. If sovereignty is violated, the operation is considered an internationally wrongful act (IWA), and therefore, gives the victim state a range of options to retaliate that it would not lawfully have if its sovereignty had not been breached (Jensen, 2016). Sovereignty is

[2] These considerations apply strictly in peacetime. When a cyber operation occurs during an armed conflict, a different legal regime applies – primarily international humanitarian law (IHL) and the law of armed conflict (LOAC) – which governs targeting, military necessity, distinction and proportionality (Schmitt, 2013).

defined as a state's exclusive authority over its territory and internal affairs according to the Permanent Court of Arbitration (1928). That same principle applies in cyberspace, almost a century later. In cyberspace, most states (although not all) argue that sovereignty extends to the infrastructure located in its territory and the activities conducted through it. Moreover, a state also holds sovereignty over its nationals and the activities they carry out overseas – for example a private company from Denmark conducting business in France (Jensen, 2016). Under the prevailing view, reflected in the positions of Germany, Switzerland, or Norway among others, cyber operations that cause physical damage, significant loss of functionality, or interfere with inherently governmental functions qualify as violations of sovereignty and therefore as IWAs (Schmitt, 2013). Espionage, which is the primary goal of most cyber intelligence operations, sits in a grey zone: espionage itself is not prohibited under international law, since most states consider it a common practice. But if the methods of an espionage operation include persistent access to government networks, disruption of state functions or any of the elements aforementioned, the majority view sees it as an IWA. These boundaries continue to evolve as states refine their legal interpretations in response to increasingly sophisticated cyber operations.

2. *Attribution*: Attribution is another main legal consideration to determine whether a state can legally retaliate against another. Under international law and the Tallinn Manual, a state is committing an IWA only if the cyber operation is attributable to it, meaning it was carried out by state organs, persons empowered to exercise governmental authority, or non-state actors who are under the effective control (fully directed) of a state. Only when attribution is established can the victim state engage in countermeasures (Fleming, 2025).

3. *Legal responses*: Once a cyber intelligence operation is attributable to a state, the Tallinn Manual dictates two lawful categories of responses available to the victim state. The first is retorsions, which are unfriendly but entirely lawful acts (such as diplomatic expulsions, economic sanctions, visa restrictions, or export controls) that do not require a prior IWA or attribution. The second is countermeasures, which are acts that would normally be unlawful but are rendered permissible because they respond to an IWA committed by another state. Countermeasures must be non-forcible, proportionate to the

injury suffered, reversible and aimed solely at inducing the responsible state to comply with its international obligations (Fleming, 2025).

In addition to these conditions, it is necessary to clarify that "retaliation" is not a technical term in international law. In this context, states use it broadly to describe any response taken after a cyber intelligence operation, but the law only recognizes retorsions and countermeasures as legitimate peacetime options. Within this peacetime framework, even when an internationally wrongful act is established, the lawful avenues available to a state almost never permit the use or threat of use of force under the UN Charter (United Nations, 1945). Resorting to force in response to a non-destructive intelligence operation would risk escalating a peacetime incident into an armed conflict, something the legal framework explicitly seeks to prevent. For this reason, this paper approaches the question of whether a state should retaliate against CYBINT operations by focusing on responses that do not escalate a non-violent incident into armed conflict. Turning an intelligence breach into a kinetic confrontation is not only unlawful, but also reckless in the current geopolitical climate unless a state faces an immediate and severe threat to its security or territorial integrity. Under the UN Charter, the use of force is prohibited, and the only exceptions (self-defense under Article 51 or previous approval from the UN Security Council), require a previous an armed attack, not CYBINT operations. Even arguments about *pre-emptive* or anticipatory self-defense rely on the old *Caroline* standard, which demands a threat that is "instant" and "overwhelming," leaving no room for delay or alternatives. CYBINT operations do not fit that threshold (Guiora, 2008). They may be hostile, intrusive, and strategically damaging, but they are not the kind of immediate threat that legally or strategically justifies force. Therefore, this analysis focuses solely on non-forcible forms of retaliation[3].

[3] Because of the unique nature of each case study, new issues have been discussed during their analyses. This legal framework explains the general guideline for states to follow in cyberspace, but given the ever-changing nature of cyber, new controversies and debates arise after every CYBINT operation, as every cyber intelligence case introduces new factual patterns, new technical methods, and new legal ambiguities.

4. Case Studies

4.1. Operation Aurora: a Chinese led economic cyberespionage operation against U.S. companies.

Operation Aurora was a coordinated cyber intrusion campaign that began in mid-2009 and continued into 2010. The attackers first conducted extensive reconnaissance to identify susceptible employees and potential access points within major U.S. companies. They then leveraged a zero-day flaw (an unpatched vulnerability) in Microsoft Internet Explorer (CVE-2010-0249), delivered through targeted spear-*phishing* emails, to compromise selected systems (NIST, 2010). Once inside, they deployed the Hydraq Trojan, a type of malware that established backdoors that allowed the operators to move laterally across internal networks, escalate privileges, and avoid detection. Through these backdoors, the attackers gained access to source-code repositories, confidential corporate communications, and trade secrets belonging to more than twenty major American firms as well as the email accounts of Chinese human-rights activists and journalists (Nasir & Sohail, 2025).

The investigation that followed quickly pointed to Chinese-linked led actors. McAfee's and other forensic investigations firms analyses revealed that the operation originated from servers based in Taiwan and China, and further digging uncovered two educational institutions in China that played a part in the infrastructure of Aurora; Shanghai Jiao Tong University and Lanxiang Vocational School, both reportedly associated with China's foreign intelligence agency, MSS and the People's Liberation Army (PLA) Unit 61398 (Nasir & Sohail, 2025). The unit has been linked to large-scale cyber espionage campaigns usually targeted at large corporations and governments such as the U.S., the U.K. and Europe, starting as early as 2006. Its operations, like Operation Aurora, are based on a cyber tactic known as APT (Advanced Persistent Threat); *phising* and exploitation of zero-day vulnerabilities consistently, establishing persistent access to networks and exfiltrating intellectual knowledge such as trade secrets or technology. The unit's activity is viewed as China's broader strategic objective of acquiring foreign technology and industrial knowledge to better their economic position against their adversaries. They are, in that regard, notoriously the best, most skilled state when engaging in cyber economic espionage operations (Ellis, 2015).

The attackers penetrated Google's internal surveillance databases, reportedly used by U.S. authorities to monitor Chinese operatives, as well as Adobe's source-code servers, gaining access to proprietary technology and confidential information. Although the total economic impact was never publicly quantified, the breach represented a loss of competitiveness for U.S. companies and millions of dollars in lost innovation and cybersecurity costs (Alperovitch, 2011).

4.1.1. U.S. Response to Operation Aurora.

The corporate losses, followed by Google's public attribution of the attack to Chinese actors, triggered a diplomatic rupture between the United States and China. Washington increased political pressure on the PRC through public statements by senior officials, including the Secretary of State, along with advisories and briefings issued by the FBI and the Department of Homeland Security. The United States also strengthened export controls and scrutiny on Chinese technology firms in the aftermath of the attack. All of these measures fall squarely under the category of retorsions and therefore remain lawful under international law (Nasir & Sohail, 2025). There is no public record of countermeasures such as retaliatory CYBINT operations against China.

The reason for this seemingly "soft" American response is rooted in that, unlike China, the United States does not engage in economic espionage to steal commercial intellectual property to benefit domestic firms. This long-standing norm in the U.S. Intelligence Community (shared by some, although not all democratic states) explains why the response to Aurora remained within the non-forcible, retorsion-focused end of the spectrum (Rovner et al., 2025). Another factor to consider is that this operation took place in 2009, at a time when cyberspace had not yet become a central concern for most Western states. Technological development was accelerating, but the integration of cyber tools with intelligence collection and military activity was still poorly understood. The capabilities and strategic implications of CYBINT were far from clear. China, however, had already begun to see the strategic value of cyber-enabled economic espionage, consistent with its early *Indigenous Innovation*[4] policies aimed at acquiring foreign technology to accelerate domestic development. In that context, Operation Aurora served as a wake-up call for

[4] Indigenous Innovation is an early-2000s Chinese policy aimed at closing the technology gap with the United States. Analysts like Chow (2013) argue that, based on the policy's wording and implementation, it effectively incentivizes Chinese firms to obtain foreign technology through economic espionage and other non-market means, lowering domestic R&D costs in the process.

the United States and its allies, demonstrating that cyberspace could become a primary arena for political, economic, and diplomatic competition where tensions could be maintained below the threshold of armed conflict (Chow, 2013).

In the longer term, the American "retaliation" or response to the lessons learned from intrusions like Operation Aurora has been a significant shift in cyber policy. In 2018, the U.S. Cyber Command (USCYBERCOM) formally introduced the "persistent engagement" strategy, built on a straightforward premise: adversaries are less able to penetrate U.S. networks if they are constantly forced to defend their own. Persistent engagement is based on the idea of "defending forward" and emerged from the realization that the United States was operating at a disadvantage in a domain where China had held the upper hand for years. It focuses on disrupting adversary infrastructure and activities before they reach American systems. Although more proactive (and offensive) than previous approaches, persistent engagement still sits firmly within the peacetime framework. It is a strategic attempt to narrow the gap with China's aggressive cyber posture while remaining inside the legal boundaries that govern state behavior in cyberspace (Healey, 2020).

4.2. Stuxnet: first case of a forceful CYBINT and military operation.

Stuxnet was the name of the malware used in a covert joint operation carried out by the United States and Israel called Olympic Games in 2010, and it was targeted against Iran's nuclear enrichment program. Intelligence collected by Mossad indicated that Iran was using the Natanz military complex as a uranium-enrichment facility, a process central to the development of nuclear weapons. A nuclear-armed Iran represented a significant security concern, particularly for Israel, given its geographic proximity and the historically adversarial relationship between the two states (Levi, 2011).

Israel's Unit 8200 and the United States' CIA and NSA collaborated to disrupt Iran's nuclear program, though the method they chose was unprecedented. They developed a piece of malware specifically designed to damage physical industrial equipment. Uranium enrichment relies on centrifuges that separate the lighter U-235 isotope from the heavier U-238. Producing weapons-grade material requires increasing the concentration of U-235, and by targeting and

degrading the centrifuges that performed this process, the malware significantly undermined Iran's ability to continue enrichment (Lindsay, 2013).

This operation required a combination of intelligence collection and military planning. First, it depended on a HUMINT source inside the Natanz facility to introduce a malware-infected USB drive capable of deploying the payload. Natanz's industrial network was almost certainly air-gapped (disconnected from any network), and the only viable entry point was to physically bridge that gap and allow the malware to propagate internally. Stuxnet did not target the centrifuges directly; it focused on the facility's Supervisory Control and Data Acquisition (SCADA) system and its Programmable Logic Controllers (PLCs). The SCADA system supervised and monitored the enrichment process, while the PLCs determined the centrifuges' spin rates, dictating when they accelerated or slowed down. By infecting Natanz's Windows systems, Stuxnet intercepted legitimate SCADA instructions and altered the PLC code to manipulate the centrifuges' spin rates, pushing them to levels that caused physical degradation beyond repair. Additionally – and this was the most sophisticated aspect of the operation – the malware was programmed to deceive the Human-Machine Interfaces (HMIs), the displays and screens used by operators to monitor the system, preventing any alarms from triggering until the centrifuges were already irreversibly damaged (Lindsay, 2013).

The immediate effect of Operation Olympic Games was the physical degradation of Iran's enrichment capability at Natanz. Estimates vary, but most sources agree that roughly one thousand centrifuges were destroyed before Iran understood that it had been attacked. This forced Tehran to replace equipment, adjust the configuration of its enrichment halls, conduct internal investigations, during which several operators were dismissed before anyone realized the system had been compromised, and reassess the security of its industrial control systems. While some analyses claim the setback to Iran's nuclear program lasted only a few months, others argue the delay could have extended into the scale of years (Kamiński, 2020).

4.2.1. Iran's response to Stuxnet.

From a legal perspective, Operation Olympic Games constitutes an internationally wrongful act. The operation produced kinetic effects, damaging industrial equipment beyond repair inside a sovereign state's nuclear facility. As mentioned before, the customary standard for anticipatory self-defense derived from the *Caroline* incident requires that a threat be instant and overwhelming, but in the case of Operation Olympic Games, there was no intelligence indicating an imminent armed attack that would satisfy this threshold. Stuxnet cannot therefore be justified under international law as an act of pre-emptive self-defense and is considered an internationally wrongful act (Guiora, 2008). Under most interpretations of international law, and according to the majority view reflected in the Tallinn Manual, this kind of physical destruction also qualifies as a use of force (Jensen, 2016). The use of force, however, does not automatically mean that an operation has crossed the much higher threshold of an armed attack. The damage inflicted by Stuxnet, while significant, was contained, limited, controlled, and produced no human casualties. This distinction is critical: only an armed attack triggers a state's right of self-defense, including the use of traditional military means (Fleming, 2025).

Iran did not respond to Stuxnet with force, despite the operation having caused physical damage to its nuclear infrastructure. Instead, Tehran's reaction stayed firmly within the non-kinetic domain. Iranian officials publicly denied the scale of the damage for months, likely to avoid signaling vulnerability (Lindsay, 2013). Once the scope of the sabotage became clear, Iran accelerated its investment in offensive cyber capabilities, building the foundations of what would become its modern cyber strategy. The outcome of Iran's reaction illustrates a broader pattern in state practice. Even when confronted with a cyber operation that causes physical damage, states remain reluctant to escalate into conventional violence. Iran chose to respond through cyber operations of its own, including the 2011-2013 distributed denial-of-service attacks against U.S. financial institutions and the 2012 Shamoon attack against Saudi Aramco, all of which remained below the threshold of armed conflict. This reflects an emerging, informal norm: even forceful cyber operations do not automatically pull states into violent retaliation. Instead, competition stays within cyberspace as a form of customary restraint that prioritizes politics and strategy over armed escalation. Stuxnet, in this sense, demonstrates how an aggressive CYBINT-linked operation can

remain contained within the non-violent peacetime framework, without triggering any violent retaliation (Farwell, 2011).

5. Key findings and conclusion

Based on the legal and case study analysis conducted, as well as research, the question about whether a state should retaliate against CYBINT operations can be answered based on these main findings:

1. Most CYBINT operations fall clearly below the threshold of an armed attack. As of today, with the exception of some very specific, episodic cases, the majority of CYBINT operations do not lawfully trigger Article 51 of the UN Charter[5].
2. States overwhelmingly choose non-forcible responses even if the CYBINT operation in question employs use of force, like in the case of Iran.
3. Retaliation in practice remains non-escalatory. States are well aware of the consequences of responding to a non-violent intelligence operation with armed force. Outside of rare, militarized cases, most CYBINT operations focus on economic or political espionage, as illustrated by Operation Aurora. Escalating diplomatic tension into open conflict is not only unlawful, but also strategically nonsensical in the current geopolitical environment (Lowenthal, 2025).

Nation states not only should retaliate against CYBINT operations, but they *must*. Failing to respond to repeated cyber intrusions signals weakness, and the international trend is clearly moving toward a more offensive use of cyberspace (USCYBERCOM's Persistent Engagement strategy is a clear example of this shift) (Healey, 2020). One of the main considerations when retaliating is the potential cascading effect and the need for proportionality. States consistently keep their disputes and countermeasures within the grey zone of cyberspace, where attribution

[5] The 2015–2016 Ukraine blackouts are viewed by some states (though not all) as qualifying for the "armed attack" threshold, given that Sandworm – a Russian military intelligence cyber unit – compromised critical infrastructure and created a risk of significant civilian harm. Each blackout lasted less than a day, and this paper does not analyze these incidents due to their exceptional nature; the aim here is to provide a broader framework for assessing retaliation in response to CYBINT operations.

remains difficult, plausible deniability[6] is common, and espionage is broadly treated as a routine element of state competition. It is largely because of this informal standard that no major global power has responded to a CYBINT operation by attacking another global power's electrical grid or nuclear facilities, for example, a nation-wide American blackout induced by Chinese hackers. Proportionality applies in cyber just as it does in armed conflict, not only for legal reasons, but for strategic ones as well (Cormac & Aldrich, 2018).

As a final note, the cases analyzed in this paper are very different both in nature and in legal status. Operation Aurora was a very successful cyber-espionage operation on U.S. firms that although unfriendly, the majority view does not consider it an IWA (Fleming, 2025). Stuxnet, on the other hand, is widely considered an IWA due to the destruction of industrial equipment and violation of sovereignty, allegedly attributable to the United States and Israel after numerous private forensic investigations (Kamiński, 2020). Despite these differences, the responses in retaliation of each of the victim states remained peaceful. Both cases ultimately point to the same conclusion: nation states should retaliate against CYBINT operations, but the form that retaliation takes must stay within the non-forcible space where states already operate. The practice of states shows that retaliation is necessary, but escalation to force is neither legally justified nor strategically sensible.

[6] Neither the United States nor Israel have ever been formally charged under international law for Stuxnet. Both states maintained plausible deniability, never publicly acknowledging responsibility, and Iran chose not to pursue any legal action through international courts or the UN system, opting instead for cyber retaliation (Lindsay, 2013).

References.

Alperovitch, D. (2011). *Revealed: operation shady RAT* (Vol. 3, p. 2011). McAfee.

Chow, D. C. K. (2013). *China's indigenous innovation policies and the world trade system.* Northwestern Journal of International Law & Business, 34(1), 81–134.

Cormac, R., & Aldrich, R. J. (2018). Grey is the new black: covert action and implausible deniability. *International affairs*, *94*(3), 477-494.

Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber.

Council on Foreign Relations. (n.d.). *Winnti Umbrella.* https://www.cfr.org/cyber-operations/2018/05/03/winnti-umbrella/

Ellis, J. M. (2015). *Chinese cyber espionage: a complementary method to aid PLA modernization* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40.

Fleming, C. (2025). *The peacetime legal framework for cyber operations: Internationally wrongful acts in cyber and lawful state responses*. NYU School of Professional Studies.

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.*

Guiora, A. N. (2008). Anticipatory self-defence and international law – a re-evaluation. *Journal of Conflict and Security Law*, *13*(1), 3-24.

Healey, J., & Caudill, S. (2020). Success of persistent engagement in cyberspace. *Strategic Studies Quarterly*, *14*(1), 9-15.

Jensen, E. T. (2016). The Tallinn manual 2.0: Highlights and insights. *Geo. J. Int'l L.*, *48*, 735.

Kamiński, M. A. (2020). Operation "Olympic Games." Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme. *Security and Defence Quarterly*, *29*(2), 63-71.

Levi, M. A. (2011). Limiting Iranian Nuclear Activities.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security studies*, *22*(3), 365-404.

Lowenthal, M. M. (2025). *Intelligence: From secrets to policy*. CQ press. https://books.google.com/books?hl=es&lr=&id=5lhMEQAAQBAJ&oi=fnd&pg=PA1962&dq=lowenthal+intelligence&ots=zE2pH_bXtn&sig=cnQNfZh9PVqPEuU682vmCmaK66A#v=onepage&q=lowenthal%20intelligence&f=false

Nasir, F., & Sohail, R. (2025). State, surveillance, and cyberspace: An intelligence analysis of Operation Aurora. *Social Science Review Archives, 3*(2), 1668–1675.

National Institute of Standards and Technology (NIST). (2010). *CVE-2010-0249*. NVD. https://nvd.nist.gov/vuln/detail/CVE-2010-0249

Nye Jr, J. S. (2010). Cyber power.

Permanent Court of Arbitration. (1928). *Island of Palmas (Netherlands v. United States).*

Rid, T. (2012). Cyber war will not take place. *Journal of strategic studies*.

Rovner, J., Cormac, R., & Maschmeyer, L. (2025). Sand in the gears: Sabotage in world politics. *European Journal of International Security*, 1-20.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

United Nations. (1945). *Charter of the United Nations*.

Waltz, K. N. (1995). Policy Paper 15: Peace, stability, and nuclear weapons. https://escholarship.org/content/qt4cj4z5g2/qt4cj4z5g2.pdf