EUROPEAN LAW & GOVERNANCE UNIVERSITY
An International University by
EPLO European Public Law Organization

ELGU Students & Alumni Policy Briefs

Title: "State's sovereignty against cyber operations under the threshold of armed attack"

Author: Natalia Jasztal

Abstract

Aggressive acts in cyberspace have become a staple tool of states' foreign policy agendas, especially when carried out below the threshold of an armed attack. This prominent characteristic of the 21st century is, however, mostly governed by 20th century international law regulations. The lack of relevant regulations and political will to regulate current cyberspace may pose a threat to states' sovereignty.

Key words: cyber operations, cyberspace, sovereignty, international law, soft law.

Introduction

Cyber operations can be defined as operations carried out in cyber space. Such operations include – among others – digital espionage, advanced persistent threat (APT), infrastructure sabotage, election interference or disinformation campaigns. Aggressive acts in cyberspace constitute a permanent characteristic of 21st century's political influence methods due to its relatively low cost, high effectiveness and constantly expanding range of possibilities, which is fueled by ongoing digitalization and the use of Artificial Intelligence. It has become a staple tool for states trying to achieve their foreign policy goals.

We can differentiate between cyber operations amounting to an armed conflict (also known as cyberwarfare) to which international humanitarian law applies according to ICRC [1] and cyber operations under the threshold of armed conflict which may fall into the so-called "legal vacuum" or "grey zone". Although the hostile activities of various states' cyberspace is a phenomenon characteristic of the 21st century, they are still subject to the "old", 20th century international law regulations. [2] This raises questions whether currently existing international regulations sufficiently protect state's sovereignty against cyberoperations that do not amount to an armed attack, and how the understanding of state's sovereignty is changing in the digital age.

Main Body

According to the Council of Foreign Relations, from 2005 to 2024, 35 countries were suspected of sponsoring cyber operations. [3] The biggest players include China, Russia, Iran, and North

[1] ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, November 2019, https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (accessed 17 Sep. 2026)

[2] Agata Małecka, 'Cyber-Operations under International Law' (2022) 3(47) *Colloquium Pedagogika – Nauki o Polityce i Administracji* 151

[3] For an overview of cyber operations from 2005 to 2024, see Council on Foreign Relations (n.d.), 'Cyber Operations Tracker', https://www.cfr.org/interactive/cyber-operations (accessed 17 Sep. 2026);

Korea who sponsored 77% of all suspected operations. Noticing the increasing threat posed by cyber operations, in 2013 the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which studies norms for responsible state behavior in cyberspace**,** concluded that international law (in particular the United Nations Charter) is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful cyberspace, while acknowledging that the principles of sovereignty and non-intervention apply to states' activities in cyberspace. [4] But international regulations seem to be fragmented, chaotic and oftentimes simply lacking enforcement.

According to article 2 of the UN Charter "(1) *The Organization is based on the principle of the sovereign equality of all its Members*", and "(4) *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*". In international law, internal sovereignty means the supreme authority within a territory or the ultimate power within that territory.[5] In practice, a breach of said principle happens when a state exercises its authority in another state's territory[6]. But it is not always easy to determine whether a cyber operation constitutes a breach of sovereignty – intruding into another country's physical space is far different from doing so in an online environment. This raises additional question of what degree, what type of intrusion and on what on-premises is sufficient to engage the principle of sovereignty.

Considering this topic remains unsettled in international law, certain soft-law instruments have been created - notably Tallin Manual 2.0. Developed by an independent group of experts under the NATO Cooperative Cyber Defence Centre of Excellence, Tallin Manual 2.0 provides a detailed examination of the international law applicable to cyber operations.[7] While assessing when a cyber-attack breaches the principle of sovereignty, experts analyzed 3 different potential consequences of said attack: "(1) physical damage; (2) loss of functionality; and (3) infringement upon territorial integrity falling below the threshold of loss of functionality [8] ", but there was no consent whether all 3 effects indicate an attack has breached country's sovereignty.

Tallin Manual 2.0 argues that a cyber operation against a private company in another country could constitute a violation of another state's sovereignty, under certain conditions. [9] Other legal scholars, however, claim the opposite - that "*if a state-sponsored cyberattack is directed at a single commercial entity such as a private bank, […] this would not engage the*

[4] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 24 Jun. 2013

[5] *Customs Regime between Germany and Austria [Advisory Opinion] [Individual Opinion of Judge Anzilotti]* 57

[6] Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House, 2 December 2019, 46

[7] Kozik, A. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

[8] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)

[9] E.g. when cyber operation interferes with inherently governmental functions.

state's inherently sovereign functions because it is a private entity rather than a whole sector falling exclusively within the government's powers[10]". Unfortunately, the second take seems to be more evident in practice.

The above-mentioned theoretical discussion has a chance to be applied in practice. One interesting case study is an ongoing investigation being conducted in Poland about the leak of personal data of almost 19 million people, including medical information, via external cyber operation. The attack targeted a private company that provides services used by many medical (including national) facilities in Poland. The cybercriminals have not been yet identified, however – due to Poland being recently regularly targeted by Russian state-linked hackers – it is possible that said attack was also conducted on behalf of Russia[11].

This attack did not cause earlier referenced physical damage or loss of functionality. It is also questionable whether it amounted to an infringement upon Poland's territorial integrity, taking into account that the target was a private company. However, many could argue that this event has caused serious non-physical consequences, which raises questions whether such effects are still relevant when assessing a potential violation of sovereignty. It also showcases that an attack on a private company resulting in breach of privacy, which is a fundamental right, could indeed constitute an attack of another state's sovereignty over data.

Conclusion(s)

International law is clearly applicable to states' activities in cyberspace, but lack of relevant regulations and political will to regulate cyberspace leaves us with general customary international law and soft law instead. Based on earlier mentioned customary law and informal guidance, it is in practice extremely difficult to assess what constitutes a cyber operation in an international environment, and when such operations amount to breach of states' sovereignty under the threshold of armed conflict. As much as soft law serves as a useful tool to conduct legal research on cyber operations that have been extremely prominent in the last couple of years, the regulatory sphere requires action to reflect the actual problems arising for the cyber space. The understanding of sovereignty is also shifting due to different reality of an online presence and therefore arising threats. As long as there is no political will and states' joint response to abide by the existing rules and regulate further, cyber operations will not only remain a major part of states' foreign influence activities, but also most likely they will be exploited and weaponized even further.

[10] Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*, Chatham House, 2 December 2019, 118

[11] Notes from Poland, 'Poland hit by theft of 19 million patients' data from medical platform' (13 August 2026), https://notesfrompoland.com/2026/08/13/poland-hit-by-theft-of-19-million-patients-data-from-medical-platform/ (18 Sep. 2026)