

CYBER ESPIONAGE

How the competition for intelligence challenges international law

Asbjørn Thranov

This report is written by Asbjørn Thranov, PhD. The report is published by DIIS.

DIIS · Danish Institute for International Studies

Gl. Kalkbrænderi Vej 51A

DK-2100 Copenhagen, Denmark

Tel: +45 32 69 87 87

E-mail: diis@diis.dk

www.diis.dk

Layout and map: Lone Ravnkilde

Cover illustration: iStockPhoto / Seamartini

Printed in Denmark by Johansen Grafisk

ISBN 978-87-7236-118-5 print

ISBN 978-87-7236-119-2 pdf

DIIS publications can be downloaded free of charge or ordered from www.diis.dk.

© Copenhagen 2023, the author and DIIS.

TABLE OF CONTENTS

Abstract	4
Introduction	5
Strategic legal options in the competition over global norms, rules and principles in cyberspace	11
Breaking the silence – the legal status of cyber espionage under international law	15
National sovereignty in cyberspace	21
Cyberspace and prohibited intervention	29
Cyber and intelligence support to Ukraine and international law	35
Conclusion	41
Notes	44

ABSTRACT

Cyber espionage has become a common method for states to gather confidential information in cyberspace. The vast interconnectedness of the Internet provides a target-rich environment for states to engage in low-risk collection of large amounts of data at an unprecedented speed and scale. Cyber espionage may look different from traditional espionage, but it is essentially an expression of the tension between competing states. States use espionage, cyber or otherwise, to strengthen their own position and security in competition with political, military, or economic rivals. In this manner, cyber espionage is best understood as an integral part of an ongoing intelligence contest in cyberspace. This report explores how international law applies to peacetime cyber espionage. By taking stock of recent legal statements by states, this report specifically examines how states have interpreted the principles of territorial sovereignty and non-intervention in the cyber context. The report also analyses the legal implications of provision of intelligence and cyber support to Ukraine by Western states.



Photo/Illustration and description: Halfpoint, Shutterstock. Hacker in military uniform on dark web, cyberwar concept.

INTRODUCTION

Cyber espionage is an ever-present phenomenon in current international affairs. The global spread of the Internet has democratised the ability of states to engage in espionage and many states now use cyberspace to collect information of political, military and economic value to further their own national interests. The low cost of entry has provided developing countries and smaller states with new and relatively cheap ways of collecting intelligence. While cyber espionage has not significantly levelled the playing field between weaker and more powerful states, high-tech espionage is no longer the exclusive province of the most powerful actors in the world. Today, cyber espionage is one of the most common forms of state-sponsored activity in cyberspace.¹

This use of a novel technology to spy inevitably raises questions about international law. How does the system of rules and principles that regulate relations between states and, increasingly, individuals and other actors in international affairs govern the practice of cyber espionage? This report explores how international law applies to cyber espionage.

The legal status of peacetime espionage under international law has long been characterised by some degree of opacity and ambiguity. There is still much uncertainty about how existing international principles apply to state cyber espionage activities. In particular, it remains unclear whether cyber espionage violates the fundamental principles of territorial sovereignty and non-intervention. However, in recent years states have begun to speak more openly about how international law applies to cyberspace. To date, around 30 states have published comprehensive legal positions on the application of international law in cyberspace.² These official articulations can help develop shared understandings and potentially, over time, could lead to the crystallisation of so-called customary international law.

Taking stock of recent state pronouncements on the application of international law in cyberspace, this report seeks to reduce the ambiguity surrounding cyber espionage by providing decision-makers, practitioners and academics with greater insight into the present legal landscape of cyber espionage under international law. To frame the discussion, this report situates cyber espionage within a conceptual understanding of state activities in cyberspace as an intelligence contest.³

BOX 1. WHAT IS CYBER ESPIONAGE?

Cyber espionage generally refers to one state hacking into another state's computer networks to gather data or to map the targeted system. The primary focus of cyber espionage is not to cause destructive or disruptive effects but to exfiltrate or copy confidential or sensitive data from the target network.

Cyber espionage is a subcategory of traditional espionage, which includes the collection of intelligence by spies (human intelligence) and interception of electronic signals (signal intelligence).

Cyber espionage is different from traditional espionage for at least three reasons:

Range

The interconnectedness of networks has given states a wide geographical reach that allows them to collect large amounts of information without physical proximity to the target. Because cyber espionage is conducted remotely, states can collect information without having to send a human spy to the target state. In theory, any computer system connected to the Internet can be accessed in a matter of seconds.

Scale

Cyber espionage enables states to gain access to large amounts of sensitive data. The surge in digitalisation has further increased the quantity of data available on the Internet. This increase in online information has enabled states to collect data at an unprecedented scale.

Low risk

Cyber espionage can be very difficult to trace back to the perpetrator due to the near-complete anonymity afforded by the Internet. States can easily hide or delete their digital traces. This relative anonymity supports deniability and can make it more difficult for the victim state to assign blame to the spying state. As a result, the political and diplomatic costs of getting caught are lower than for other, more traditional, forms of espionage.

Cyber espionage is an integral part of the intelligence contest

The term 'cyber war' is often used to describe states' activities in cyberspace. However, 'cyber war' is a rather imprecise and misleading label. It implies that states use cyberspace as a new battlefield to conduct destructive and disruptive cyberattacks against each other in a warlike scenario. Although states do use cyber operations at times of armed conflict, as seen in the Russo-Ukraine war, the vast

majority of cyber operations occur below the level or outside the context of armed conflict. Rather, cyberspace has become an arena for competition between states. This political reality has led some scholars to characterise states' activities in cyberspace as an intelligence contest rather than a 'cyber war'.⁴ According to the American intelligence scholar Joshua Rovner this contest entails five elements:

First, it is a race among adversaries to collect more and better information. Second, it is a race to exploit that information to improve one's relative position. Third, it is a reciprocal effort to covertly undermine adversary morale, institutions, and alliances. Fourth, it is a contest to disable adversary capabilities through sabotage. Fifth, it is a campaign to pre-position assets for intelligence collection in the event of a conflict.⁵

From this perspective cyber espionage is more than merely information gathering and rarely an end in and of itself.⁶ Rather, it has become a central tool of statecraft in global geopolitical competition for power and influence.⁷


States use cyber espionage to gain an information advantage or even information superiority over competitors to advance their national interests and to improve their relative power position on the international stage. In its 2022 annual threat assessment, the Danish Defence Intelligence Service predicted that as 'the competition intensifies between state actors, rival states will increasingly try to steal information through espionage, in particular cyber espionage'.⁹ Similarly, in a speech in 2022 to the Dutch Military Intelligence and Security Service (MIVD) the Dutch Minister of Defence, Kaja Ollongren, noted that '[h]ostile hackers move virtually at lightning speed, from server to server, from country to country, with new attack methods and the use of new technology. In this ongoing intelligence contest, it is up to the MIVD to [...] keep an eye on it'.⁹

Given that some states view cyber espionage through a competitive lens, the concept of the intelligence contest provides a useful analytical framework to understand digital spying.

While this intelligence contest primarily occurs below the threshold of armed conflict, it is not only a peacetime competition. The Russo-Ukrainian war clearly illustrates the intelligence contest being played out in the context of a war. Western states have

increasingly relied on deliberate public disclosure of intelligence information as an instrument to influence public opinion and inform political decision-making.¹⁰ Moreover, some states have provided various forms of cyber support to Ukraine. In addition, states have also shared classified intelligence with Ukraine to support military efforts. Yet, by providing this support to Ukraine, Western states risk breaching their neutrality obligations or even becoming party to the conflict alongside Ukraine.

The growing importance of cyber espionage as a tool of international competition and conflict raises novel legal questions about the role that international law and norms play in the intelligence contest in cyberspace. The focus of this report is on whether international law imposes any legal constraints on states' cyber espionage activities in the intelligence contest between states in cyberspace.



States use cyber espionage to gain an information advantage or even information superiority over competitors to advance their national interests and to improve their relative power position on the international stage.

Structure of the report


Following this brief introduction, the chapter 'Strategic legal options in the competition over global norms, rules and principles in cyberspace' provides a general assessment of the strategic legal options that states have with respect to their position on how international law applies in cyberspace. The chapter 'Breaking the silence – the legal status of cyber espionage under international law' discusses the legal status of peacetime espionage under international law and concludes that the legality of cyber espionage must be measured against general international law and existing instruments. On this basis, the chapter 'National sovereignty in cyberspace' examines whether, and if so under what circumstances, the fundamental principle of territorial sovereignty imposes any legal constraints on states' cyber espionage activities. The chapter 'Cyberspace and prohibited intervention' examines whether cyber espionage amounts to unlawful interference in another state's internal affairs. The chapter 'Cyber and intelligence support to Ukraine and international law' shifts the focus away from how intelligence is collected in peacetime by cyber means and examines the legality of Western states providing Ukraine with cyber support and intelligence information. The final chapter offers conclusions and some perspectives on the role of cyber espionage in the world of today.



Photo/Illustration and description: Siberian Art, Shutterstock.
Vector polygonal art style human hand.

STRATEGIC LEGAL OPTIONS IN THE COMPETITION OVER GLOBAL NORMS, RULES AND PRINCIPLES IN CYBERSPACE


The intelligence contest in cyberspace is not only a geopolitical competition between states over information; it is also a competition over the global norms and international rules that govern, or should govern, state activities in cyberspace.¹¹ The legal uncertainty surrounding general international rules and principles is magnified in the cyber context. States have competing views of how existing norms, rules and principles should guide behaviour in cyberspace. This norm competition is only likely to increase in the near future with different actors competing to form the normative and legal landscape in cyberspace.¹² As a result, the intelligence contest is conducted in a legal environment marked by unsettled global normative consensus. The analogy is, simply put, like a game of chess, but one where the rules of the game are unclear, and even where clear, are not always embraced by the players.



The intelligence contest in cyberspace is not only a geopolitical competition between states over information; it is also a competition over the global norms and international rules that govern, or should govern, state activities in cyberspace.

States can, broadly speaking, pursue three different strategic routes in this norm competition.¹³ The options are essentially a choice between (1) clarity, (2) ambiguity, or (3) silence regarding the interpretation of international law in the cyber context.

Clarity: Some states may consider that international law can act as a deterrent against hostile cyber operations by other states. The rationale is that international law is an important tool to deter such hostile cyber activities, as victim states can condemn the behaviour of other states. For international law to have its full deterrent effect, the rules must be relatively clear and straightforward. Clear rules also allow states to engage in legal responses to unlawful conduct by other states. States taking this view want international law to be clear and restrictive and to limit state operations in cyberspace.¹⁴ This approach might be favoured by smaller states and developing countries with insignificant or weak cyber capabilities. By contrast, clarity may be less favoured by more powerful states with developed cyber capabilities. These actors may seek to deter other states' cyber espionage activities through the threat of retaliation with so-called 'hack backs' that would violate the sovereignty of the spying state. Greater legal clarity might limit their ability to respond with these forms of active cyber defence operations, and thus limit their ability to deter other states' cyber espionage.¹⁵



Powerful cyber actors may favour ambiguity and uncertainty with respect to how international law applies in the cyber context. Legal ambiguity affords these states the advantage of operating in a legal grey zone, where the precise contours of the rules are difficult to discern.

Ambiguity: Powerful cyber actors may favour ambiguity and uncertainty with respect to how international law applies in the cyber context. Legal ambiguity affords these states the advantage of operating in a legal grey zone, where the precise contours of the rules are difficult to discern.¹⁶ Ambiguity may also provide these states with some operational flexibility as it leaves them with increased scope for action in the cyber context.¹⁷ Legal ambiguity also creates a deterrent value for these cyber-capable states, as they can respond with low-intensity cyber operations against the spying state as mentioned above. As a result, cyber-capable states may resist greater clarity about the rules, and instead seek to exploit the normative ambiguity to advance their national interests. In short, ambiguity can be said to favour powerful states and disadvantage weaker states.

Silence: Yet other states remain completely or partially silent on how international law applies to state activities in cyberspace. Silence may be a strategic choice of states to enable greater legal room for manoeuvre when pursuing their activities in cyberspace. Or they may be reluctant to offer their own views for fear that this could expose some legal vulnerabilities that might be exploited by other states. Some states simply remain silent because they lack the governmental expertise to understand the technical and legal complexities surrounding state activities in cyberspace.¹⁸ Finally, states may also remain silent to avoid choosing a side in a contested legal debate, which is largely dominated by blocs of global and regional powers.

Given the importance of cyberspace and the rapid development of technology, states are increasingly faced with different legal strategic options when assessing the applicability of international law to cyberspace. While states might prefer one legal strategy over another, they appear to carefully balance their national interests by combining all three strategies at once. Given the rapid technological development in cyberspace, this measured and careful approach may be the most desirable for most states.



Source: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions

BREAKING THE SILENCE – THE LEGAL STATUS OF CYBER ESPIONAGE UNDER INTERNATIONAL LAW

The legal status of peacetime espionage under international law has long been relatively unsettled. While espionage is criminalised by most states in their national legal systems, it is not directly and specifically prohibited by international law. There is no international treaty that prohibits espionage. Moreover, international courts have never concluded that spying in and of itself is unlawful under international law.

The ambiguous legal status of espionage is not only a cyber issue, but also applicable to other forms of foreign intelligence collection outside the cyber domain.¹⁹ Although espionage is a common practice, states have traditionally been reluctant to express their legal views on whether international law imposes any constraints on spying

between states. However, in recent years states have broken this silence, and have increasingly begun to speak out on the legal status of cyber espionage under international law.

A dominant view in the academic literature is that international law does not prohibit espionage as such, but that specific rules and principles regulate the means and methods states use to collect intelligence.²⁰ In other words, states are freely permitted to conduct espionage unless their spying activity contravenes specific international rules (for example, diplomatic law protecting official correspondence of diplomats).²¹


Several influential cyber powers have separated themselves from other states in their willingness to speak about the legal status of cyber espionage:

- The **United States** has expressly mentioned that ‘there is no per se international legal prohibition’ against espionage.²² According to the American view ‘[t]here is no anti-espionage treaty, and there are many concrete examples of States practicing it, indicating the absence of a customary international law norm against it’.²³
- **Canada** has noted that, ‘espionage, while not per se wrongful under international law, could be carried out in a way that might violate international law’.²⁴
- **France** also observes that, ‘cyber espionage[...] is not illegal in international law, though it may infringe such law when linked with an internationally wrongful act’.²⁵
- **Norway** is also of the view that, ‘cyber espionage, that is cyber operations whose purpose and effect is limited to the mere collection of information for use by the authorities, is not in itself illegal under international law. However, certain aspects of such intelligence operations could violate specific rules of international law’.²⁶
- The **United Kingdom** takes the position that, ‘more routine and legitimate information gathering [is] carr[ied] out as part of international relations’.²⁷ More pointedly, the Director of Legal Affairs to the UK Government’s Communications Headquarters (GCHQ) has in his official capacity proclaimed that, ‘espionage, more generally, is not considered to be a violation of international law by pretty much every state’.²⁸
- **Costa Rica** has recently suggested that ‘[s]urveillance operations may be carried out in ways that lead to breaches of State or other rules of international law’.²⁹

These statements carry persuasive legal support for the position that espionage, cyber or otherwise, does not violate international law, but that the means, methods and effects of how information is collected might do. Thus it can be said that cyber espionage is regulated by international law, but only at the margins.

One should, however, be careful to conclude that this position is universally accepted by all states. While states may accept that espionage is a reality of international affairs, this does not mean that all states view spying as legal under international law.³⁰ Sometimes states protest against espionage activities with direct reference to international legal rules. This was for instance the clear case in 2013, where the member states of the Union of South American Nations (UNASUR) condemned the United States' global espionage in a statement to the United Nations. According to the statement, 'the interception of telecommunications and espionage actions[...] constitutes a threat to security and serious violations of human, civil and political rights, of international law and of national sovereignty, and [...] damages relations among nations'.³¹ This statement was in reaction to the revelations made by Edward Snowden, a former employee of the National Security Agency (NSA), that the United States had conducted global technical espionage against friends and foes.

However, generally states are reluctant to invoke the language of international law when condemning another's cyber espionage operations. The reason for this is simply that a legal condemnation would often also apply to the target state's own practices of spying.



It is doubtful whether there is sufficiently widespread and consistent state practice and opinio juris to conclude that customary international law generally prohibits economic cyber espionage.

To avoid accusations of hypocrisy, the spied-on state will typically respond to another state's cyber espionage with acts of retorsion such as diplomatic or economic sanctions that, while unfriendly, are not inconsistent with the state's international obligations. Retorsion may be a useful response to cyber operations that are not unlawful per se under international law such as cyber espionage. Although acts of retorsion are an available response option for all states, they are likely most effective when imposed by a powerful state with the resources to mitigate the potential political or economic cost.

Moreover, some states might view cyber espionage as an illegal practice under international law although they remain silent on the topic. This silence cannot be assumed to constitute acquiescence or implied consent that espionage is legal.³² That said, some academic commentators remain overly focused on the issue of state silence regarding the legal status of cyber espionage, rather than turning their attention to recent national statements that do expressly deal with this question.³³ As will be shown as this report progresses, several states have articulated clear positions on legal matters surrounding cyber espionage. In other words, several states have broken their policy of silence on cyber espionage and international law.

Finally, it should be noted that although the United States and individual European states generally consider cyber espionage to be lawful under international law, the same states have advocated for a political norm prohibiting economic cyber espionage for commercial purposes. However, this norm is merely a non-binding social norm that has never developed into a legally binding rule. Moreover, this social norm has never gained universal acceptance in the international community, and today, it is largely seen to have failed (see Box 2).

BOX 2. THE FAILED NORM AGAINST ECONOMIC CYBER ESPIONAGE

States are increasingly turning to cyberspace to collect intellectual property, and to trade secrets and other sensitive information from foreign companies. This information is then used to provide competitive advantages to the spying state's domestic private companies. This form of espionage is often classified as economic cyber espionage and is distinguished from cyber espionage for national security purposes. Economic cyber espionage appears to be a very central part of some states' participation in the intelligence contest. Most notably, China is often accused by Western states of engaging in large-scale economic cyber espionage.³⁴

International law does not prohibit economic cyber espionage for commercial purposes. But the United States and other Western states have sought to promote an international, non-binding norm prohibiting economic cyber espionage.³⁵ This norm first emerged in the 2015 bilateral cyber agreement between China and the United States.³⁶ China also made similar bilateral agreements with Australia, Canada and the United Kingdom not to steal confidential information from private companies.³⁷

The norm was later endorsed by the G-20 countries agreeing in 2015 that 'no country should conduct or support ICT-enabled³⁸ theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors'.³⁹

Western states supporting this norm have argued that there is sufficient state practice and legal belief (*opinio juris*) to generate a new, legally binding, customary norm that prohibits economic cyber espionage. For instance, Norway claimed in the preparatory work to the Norwegian intelligence act that the prohibition against economic espionage has crystallised in customary international law.⁴⁰

However, it seems clear that an international norm against cyber espionage has never been universally accepted by most states in the world. China and other states continue to conduct economic cyber espionage. Therefore, it is doubtful whether there is sufficiently widespread and consistent state practice and *opinio juris* to conclude that customary international law generally prohibits economic cyber espionage.



Photo/Illustration and description: Vit-Mar, Shutterstock.com.
Map of the planet, futuristic background. Global social network.


NATIONAL SOVEREIGNTY IN CYBERSPACE

Sovereignty has potential important implications in the context of the intelligence contest. The principle generally refers to states' authority to control matters within their jurisdiction and to their right to conduct foreign relations with other states. A sovereign state also has the right to not have its territorial integrity violated by other states.

Historically, sovereignty has been strongly oriented towards territory and geography. However, territorial borders do not exist in cyberspace. State cyber activities often transcend the geographical boundaries of countries. The borderless nature of

cyberspace raises the question of whether, and if so when and how, the principle of territorial sovereignty applies in the cyber context. This question is hotly debated among states and by academics.

It has been argued that sovereignty is merely a political principle of international relations rather than a binding international legal rule. From this perspective sovereignty does not operate as a standalone rule that can be independently violated by state cyber activities. Rather, sovereignty is viewed as a baseline principle that underpins other rules of international law such as the prohibition of the use of force and the prohibition of intervention. From this angle, any digital intrusion into another state's cyber infrastructure below the level of prohibited intervention is lawful. So far, the United Kingdom is the only state that has advocated this position.⁴¹



The borderless nature of cyberspace raises the question of whether, and if so when and how, the principle of territorial sovereignty applies in the cyber context.

Instead, most states that have articulated their legal position have adopted the view that sovereignty operates as a standalone rule of international law. This position is expressly adopted in national statements by e.g. Brazil,⁴² Canada,⁴³ China,⁴⁴ Costa Rica,⁴⁵ the Czech Republic,⁴⁶ Denmark,⁴⁷ Finland,⁴⁸ France,⁴⁹ Germany,⁵⁰ Iran,⁵¹ Ireland,⁵² Italy,⁵³ Japan,⁵⁴ the Netherlands,⁵⁵ New Zealand,⁵⁶ Norway,⁵⁷ Poland,⁵⁸ Romania,⁵⁹ Sweden,⁶⁰ and Switzerland.⁶¹ In this view, a state's remotely conducted cyber operations against another state's cyber infrastructure can amount to a violation of sovereignty and thus constitute an internationally wrongful act.


With this near consensus that sovereignty does operate as a rule that can be violated, the discussion has instead turned to the important question of when a remotely conducted cyber operation violates the rule of sovereignty. Here states have taken two different positions.

The first position is that any unauthorised intrusion into a state's computer systems would constitute a violation of sovereignty. Iran⁶² and France⁶³ have most clearly expressed this position. Under this approach, a cyber operation that is carried out on or through cyber infrastructure located in the territory of another state amounts to a sovereignty violation. This conception of cyber sovereignty is analogous to how states traditionally understand sovereignty in the real world. In the physical context,

a sovereign state has the right to not have its territorial integrity violated through non-consensual physical intrusions of their national air space, territorial waters, or land territory by other states. This view has led some scholars to argue that the principle of sovereignty provides the same protection against unconsented-to virtual intrusions as it affords the physical territory against state intrusions.⁶⁴

Conceptually, the logic behind this argument appears intuitive. It is indeed difficult to see why a remote-access cyber operation should be treated differently from an intrusion that involves a physical trespassing of another state's territory. The fact of the matter is, however, that the cyber domain is by its very design different from the physical domain. Many states have therefore developed a cyber-specific interpretation of when a state's sovereignty is violated, which differs from the traditional, territorial view of sovereignty.

The second position is that only cyber operations that produce certain harmful effects on the targeted system constitute a violation of sovereignty. This stance is for instance taken by Canada,⁶⁵ the Czech Republic,⁶⁶ Denmark,⁶⁷ and Finland,⁶⁸ to mention a few. In this view a cyber operation that results in physical damage or injury in another state qualifies as a violation of sovereignty. A case in point would be a cyberattack against a power turbine that causes it to spin out of control and subsequently catch fire.



Many states have therefore developed a cyber-specific interpretation of when a state's sovereignty is violated, which differs from the traditional, territorial view of sovereignty.

In addition to physical damage, some states have also coalesced around the view that a cyber operation that causes loss of functionality to the target cyber infrastructure may constitute a violation of sovereignty, if it reaches a certain threshold.⁶⁹ For example, the use of so-called 'wiperware' that prevents the functionality of a computer system, whether temporarily or permanently, by deleting the operating system, could constitute a violation of the target state's territorial sovereignty.

Some states have also adopted the view that sovereignty may also be violated by a cyber operation that interferes with, or usurps, an 'inherently governmental function' of the target state.⁷⁰ This basis for a sovereignty violation was suggested by the

influential Tallinn Manual 2.0. According to the manual, ‘inherently governmental functions’ are those activities that a state alone has the authority to carry out, such as administration of elections or law enforcement.⁷¹

On this basis a sovereignty violation occurs regardless of whether a cyber operation results in any physical or functional effects. Similarly, this understanding of sovereignty does not require that the interference rise to the level of coercion (which is the case with the prohibition of non-intervention, see below). For example, a cyber operation that interrupts the conduct of an election by deleting or altering voter data would constitute interference with the governmental functions of the victim state. An example of usurpation of governmental functions is the unauthorised remote law enforcement search of databases located in another state’s territory to collect evidence for criminal proceedings. The distinction between the collection of intelligence information and of evidence may sometimes be blurred in practice but is often carried out by different agencies such as external and internal intelligence services with different tasks.

In sum, most states that have articulated their view on the principle of territorial sovereignty in cyberspace agree that sovereignty is a binding rule of international law applicable to cyberspace. As such, the real division between states is not about sovereignty’s legal status, but instead about what types of remotely conducted cyber operations breach territorial sovereignty.

Cyber espionage and sovereignty

Given the above, an important international legal question in the context of the intelligence contest is whether cyber espionage is a violation of sovereignty. A growing number of states have begun to express their official views on how international law applies to cyber espionage. At this stage, three dominant blocs of states have been particularly vocal in the debate about whether cyber espionage violates the principle of sovereignty.

These blocs are centred around (1) the so-called ‘Five Eyes’ intelligence alliance between Australia, Canada, New Zealand, the United Kingdom and the United States, (2) the BRICS countries, which currently consist of Brazil, India, China, South Africa and Russia, and (3) Continental European states. These global and regional groups of states are undoubtedly some of the most powerful actors with respect to the intelligence contest in cyberspace. Even though all states have a voice in clarifying how international law applies to cyberspace, it seems particularly relevant to survey the positions of these three groupings on cyber espionage and the principle of sovereignty.

'Five Eyes' intelligence alliance

The 'Five Eyes' states have adopted the position that cyber espionage does not breach the territorial sovereignty of the target state. This view has been expressed most clearly by Canada and New Zealand. According to Canada, 'cyber espionage, do[es] not amount to a breach of territorial sovereignty, and hence to a violation of international law'.⁷² New Zealand similarly makes it clear that '[t]here is a range of circumstances – in addition to pure espionage activity – in which an unauthorised cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful'.⁷³ The US has also alluded to a similar position, noting that 'international law [...] does not prohibit espionage per se even when it involves some degree of physical or virtual intrusion into foreign territory'.⁷⁴ The UK does not consider cyber espionage a violation of territorial sovereignty because such a rule does not exist in international law. Australia is the only member of the 'Five Eyes' alliance that has not expressly stated its view on whether cyber espionage constitutes a violation of sovereignty but would likely adopt the same position as its 'Five Eyes' partners due to the close cooperation.

The consensus among the 'Five Eyes' that the principle of sovereignty does not prohibit cyber espionage comes as no surprise as these states are widely believed to have the most robust and sophisticated cyber and intelligence collection capacities in the world. Therefore, these countries have a strategic interest in proffering a permissive interpretation of the principle of sovereignty in the cyber context.

BRICS

Several of the BRICS member states consider that cyber espionage violates the principle of sovereignty. China and Brazil have offered the most explicit views on the topic.

According to China, it is a violation of the principle of sovereignty, when a state conducts an 'unauthorised penetration into the network systems in the territory or within the jurisdiction of another State[...]'.⁷⁵ Moreover, China specifically mentions that '[n]o State shall engage in ICT-enabled espionage or damages against other States, including mass surveillance and theft of important data and personal information'.⁷⁶ This position is consistent with China's use of the term 'cyber sovereignty' to describe the idea that states should have a right to control access to the Internet within their territorial borders.

The Chinese view that cyber espionage violates the principle of sovereignty apparently contradicts China's own practice of spying in cyberspace. According to Western intelligence services, China is increasingly using cyber espionage to collect information of political, military and economic value from other states.⁷⁷ China may nevertheless hold the view that cyber espionage violates the principle of territorial sovereignty as a matter of law, but still, for whatever political or strategic reasons, be willing to conduct cyber espionage even though it directly contradicts its own legal interpretation of sovereignty.

Since the Edward Snowden revelations Brazil has been a major proponent of the view that cyber espionage and other forms of intelligence surveillance are a violation of sovereignty.⁷⁸ Brazil has recently affirmed this view stating that '[i]nterception of telecommunications, for instance whether or not they are considered to have crossed the threshold of an intervention in the internal affairs of another State, would nevertheless be considered an internationally wrongful act because they violate state sovereignty'.⁷⁹ This view is also supported by other Latin American countries.

Costa Rica has most clearly stated that it 'believes that, in some circumstances, cyber espionage may amount to a breach of State sovereignty'.⁸⁰ Costa Rica does not specify in detail the precise circumstances in which cyber espionage may violate the principle of sovereignty. Instead, it leaves open the possibility of taking a case-by-case approach to assessing whether cyber espionage might constitute a sovereignty violation. In doing so, Costa Rica may deliberately seek to deter other states from spying against the country by making it unclear where the exact threshold for a breach lies. Although Costa Rica is neither a cyber power nor a powerful state, its statement may carry some legal weight, as the country was the victim of a large-scale ransomware campaign in 2022 that paralysed important national cyber infrastructure.⁸¹


Russia has not expressed a similarly clear position on whether cyber espionage or other forms of low-level cyber operations constitute a breach of sovereignty. However, in 2014, Russian president Vladimir Putin declared that cyber espionage is 'a direct violation of the state's sovereignty, an infringement on human rights and an invasion of privacy' in a reaction to Edward Snowden's leaks about the United States' global intelligence programmes.⁸² If Putin's statement is taken at face value, it appears to indicate that Russia views cyber espionage as a breach of the principle of sovereignty. Thus, Putin's proclamation can also be seen as an expression of Russia's view on cyber sovereignty as a state's right to have control over information and telecommunications infrastructure within its own territory.⁸³

Neither India nor South Africa have articulated clear views on whether cyber espionage or other low-intensity cyber operations violate the sovereignty of another state. Thus, it remains to be seen whether these two regional powers consider cyber espionage to be compatible with the rule of sovereignty.

Continental European states

Continental European states have generally not offered any explicit positions on whether cyber espionage violates the principle of sovereignty.

France's position on sovereignty appears to suggest that any penetration of French computer systems would constitute a breach of sovereignty. This position would arguably render all forms of cyber intrusion unlawful, including cyber espionage aimed at collecting information. By contrast, most European states that have spoken about sovereignty in cyberspace would likely not consider cyber espionage a violation of sovereignty unless the operation also produces some sufficiently serious harmful effects on the targeted cyber infrastructure. As cyber espionage merely involves the collection of data, it will typically not cause any damage or loss of functionality to the target system.



An overwhelming majority of Western states have embraced the view that remote-access cyber espionage does not breach the principle of sovereignty. This view is not, however, widely shared by states in the Global South nor by leading members of the BRICS organisation.

Some European states have adopted the position that interference with or usurpation of a state's inherently governmental functions may constitute a breach of sovereignty. Seen from this approach, cyber espionage will likely not amount to a sovereignty violation.⁸⁴ The aim of a cyber espionage operation is not to impair the ability of the victim state to perform its inherently governmental functions, but merely involves the collection of intelligence. One exception is Poland, which suggests that at least some cyber operations that involve 'theft' of government data belonging to state organs may constitute a violation of the principle of sovereignty.⁸⁵ In doing so, Poland seems to indicate that cyber espionage against certain types of confidential data may potentially violate its sovereignty. If this reading is correct, Poland separates itself from other European states in its position on whether cyber espionage interferes with inherently governmental functions.

The survey above illustrates that there is uncertainty about whether, and if so under what circumstances, cyber espionage violates the principle of territorial sovereignty. An overwhelming majority of Western states have embraced the view that remote-access cyber espionage does not breach the principle of sovereignty. This view is not, however, widely shared by states in the Global South nor by leading members of the BRICS organisation. With the expansion of BRICS to include new members, the views on territorial sovereignty in cyberspace could become even more fragmented between blocs of states in the future. In other words, the jury is still out as to whether cyber espionage constitutes an unlawful breach of sovereignty.




Photo/Illustration and description: Illus_man, Shutterstock.com
Businessman hand, dominos effect.

CYBERSPACE AND PROHIBITED INTERVENTION

States constantly seek to influence, persuade and criticise each other. This is a ubiquitous feature of international relations. Cyberspace has provided states with new possibilities to exert influence outside their own territories.

The principle of non-intervention establishes that a state must not interfere coercively in the internal or external affairs of other states. In this manner, the rule seeks to create a distinction between permissible, but perhaps unwelcome, political influence and unacceptable intervention in the affairs of other states. This makes the non-intervention principle particularly relevant in the context of the intelligence contest, where states may seek to 'covertly undermine adversary morale, institutions, and

alliances'.⁸⁶ Thus, the principle of non-intervention could potentially set some legal boundaries for state cyber activities and prevent interstate disputes that result from the intelligence contest in cyberspace.



States constantly seek to influence, persuade and criticise each other. This is a ubiquitous feature of international relations. Cyberspace has provided states with new possibilities to exert influence outside their own territories.

The existence of the customary prohibition of intervention is well-settled in international law. Moreover, states have acknowledged that the principle of non-intervention applies to their activities in cyberspace.⁸⁷

The prohibition of intervention is generally understood to include two elements: (1), the action must bear on matters in which a state is permitted to decide freely under the principle of sovereignty; and (2) it must be coercive in nature. These two constitutive elements have authoritatively been confirmed in the 1986 judgment of the International Court of Justice (ICJ) in *Nicaragua v. United States*.⁸⁸

The element of the *domaine réservé*

The term *domaine réservé* (reserved domain) is often used to describe those matters on which a state may decide freely under the principle of sovereignty. The *domaine réservé* consists of those areas of activity that international law leaves to states, and which remain under the exclusive domestic jurisdiction of states.⁸⁹ This means that the scope of the *domaine réservé* has a dynamic nature, which can be limited based on the international obligations undertaken by a state. Put differently, if a matter is regulated by international law, a state no longer has exclusive authority to regulate over those matters. For example, international human rights law limits states' rights to control the dissemination of content online and free speech. However, even if a matter is regulated by international law, and thus no longer within the exclusive regulatory authority of the state, this does not mean that other states can impose decisions or dictate conduct with respect to those affairs.⁹⁰

BOX 3. STATE ACTIVITIES FALLING WITHIN THE DOMAINE RÉSERVÉ



Elections and democratic process



National security and stability



Healthcare and public services



Critical infrastructure, incl. energy, TV, radio and Internet



Financial systems



Education



Foreign policy and international negotiations

States have in recent years provided illustrative examples of specific activities that fall within a state's *domaine réservé* in the context of prohibited intervention in cyberspace (see Box 3). Cyber operations are typically directed against targets that fall within these broad categories. However, it is not the physical target of the cyber operation that must fall within the *domaine réservé*, but rather the area of activity that the cyber activity is meant to affect.⁹¹ Therefore, the mere fact that a cyber operation targets another state's governmental computer systems is not necessarily enough to bring the matter within the *domaine réservé*.⁹²

The element of coercion

Coercion is the second element of prohibited intervention. There is no universally recognised definition of 'coercion' in international law. Yet, in the cyber context, two types of coercion have emerged.

Under the first approach, an act is coercive when it seeks to compel a state to change its freedom of choice with respect to a matter falling within its *domaine réservé*. Under this definition, the coercive behaviour manifests when it seeks to induce a particular act or omission by the target states (i.e. 'do x, or y will happen'). To illustrate, a cyber operation that seeks to manipulate election results would deprive the target state its freedom of choice. This conventional understanding of coercion is reflected in several national statements, e.g. Brazil,⁹³ Denmark,⁹⁴ Italy,⁹⁵ and the Netherlands.⁹⁶

Under the second approach, an act is coercive when it deprives a target state's freedom of control over matters falling within its *domaine réservé*. For example, a cyber operation that prevents a hospital computer system or energy supply system from functioning would be coercive. This broader understanding of coercion is supported by Australia,⁹⁷ New Zealand,⁹⁸ and the United Kingdom.⁹⁹ By contrast, the United States appears critical towards this approach because 'focusing solely on deprivation of control, without more, could turn any disruptive cyberactivity by a State that affects, even unwittingly, certain elements of another State's activities into an unlawful intervention'.¹⁰⁰ The broad interpretation of coercion expands the scope of the non-intervention principle as it does not require that a state is forced to act or not act in a particular way.

Thus, the difference between the freedom of choice and the freedom of control approaches is essentially that the mere deprivation of control over matters falling within a state's *domaine réservé* could constitute a prohibited intervention. As such, the freedom of control approach is broader as the targeted state does not need to show that a specific cyber operation was actually or potentially compelling the target state's policy choices. This broad account of coercion could be said to be more up to date with the modern-day digital reality, where a state may seek to exert pressure on another state by taking control over its critical infrastructure with cyber means.


It is widely held that the element of coercion also entails a requirement of intent. For instance, a state-sponsored cybercrime operation that is purely motivated by financial gain lacks the required coercive intent and would not qualify as prohibited intervention. In other words, the goal of the intervention must be to change the behaviour of the target state. Yet, it might be difficult in practice to prove that a specific cyber operation was meant to interfere with the target state's decision. But as New Zealand points out in its national statement, 'intention may in some circumstances be inferred from the effects of cyber activity'.¹⁰¹

Whether an act of intervention must succeed for the act to violate the prohibition on intervention is an unsolved question. Imagine, for instance, that a robust and resilient cyber power thwarts another state's attempt to affect the target state's ability to conduct an election by targeting electoral infrastructure with cyber means. In this case the cyber operation would not violate the prohibition of non-intervention on the basis that it was unsuccessful. As a result, the victim state would be precluded from responding with lawful countermeasures and from calling out the violation. This interpretation of the rule of non-intervention could, as the United States has pointed

out, have ‘paradoxical results’;¹⁰² the paradox being that a cyber operation can be at the same time an unlawful intervention (if the victim state is not capable of defending itself), as being a lawful one (if the target state renders the operation unsuccessful).

Cyber espionage and non-intervention

In the context of the intelligence contest, the question is whether the collection of information from another state by cyber means violates the non-intervention principle. For cyber espionage to amount to a prohibited intervention, the operation would need to target policy choices falling within the *domaine réservé*, and to involve coercion.



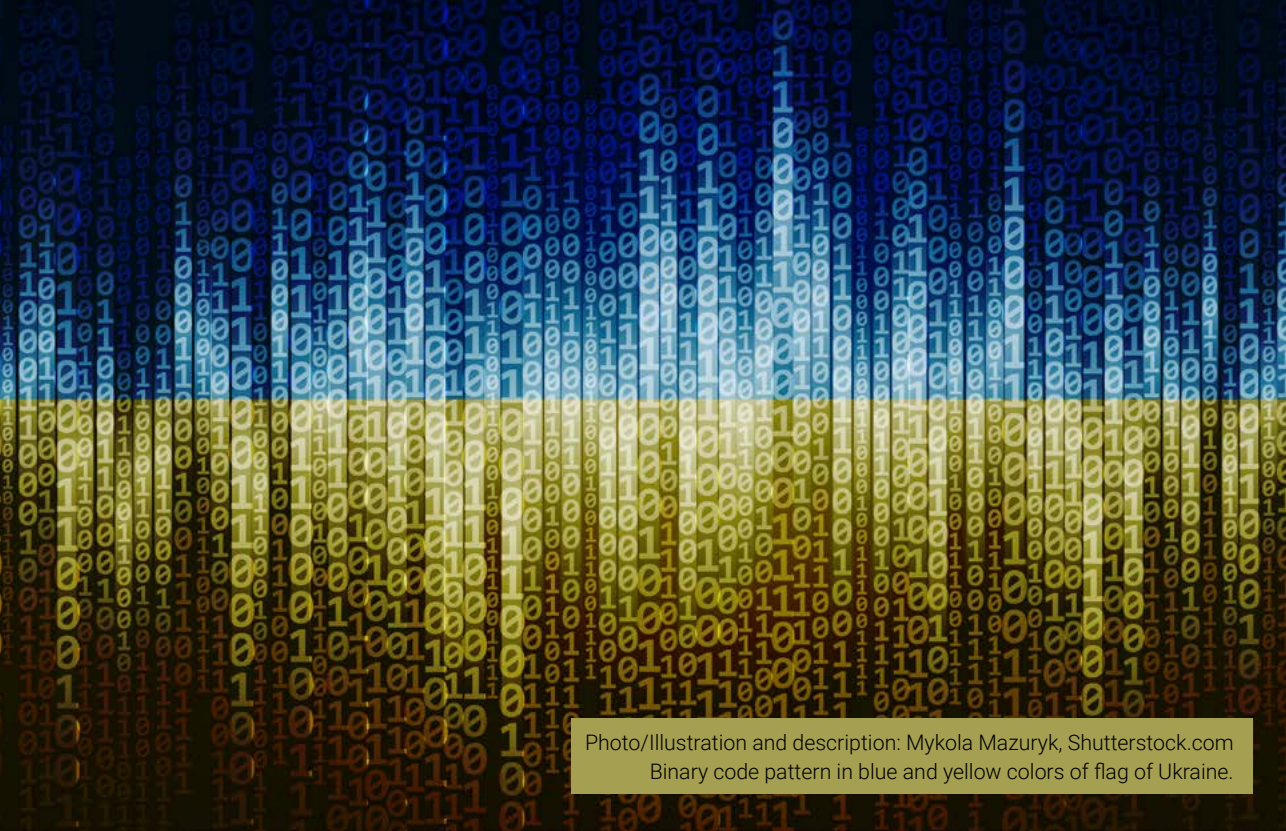
Current state practice also indicates that cyber espionage does not constitute prohibited intervention. States that have expressed their legal position on intervention in the cyber context have not mentioned cyber espionage as an example of prohibited intervention.

Although cyber espionage operations are typically directed against government IT-systems, the mere collection of information from these systems does not influence policy choices falling within the *domaine réservé*. As mentioned above, it is not the target of the cyber operation that must fall within the *domaine réservé*, but rather those matters that states are freely able to determine by their sovereignty. Cyber espionage, without more, is not designed to affect any policy choices of the target state. Moreover, cyber espionage is not coercive. The mere collection of secret information is not intended to deprive the target of its ability to control, decide, or govern matters in which it has a free choice. Therefore, cyber espionage will normally not amount to prohibited intervention as the mere collection of information is not coercive vis-à-vis the *domaine réservé*.

Current state practice also indicates that cyber espionage does not constitute prohibited intervention. States that have expressed their legal position on intervention in the cyber context have not mentioned cyber espionage as an example of prohibited intervention. On the contrary, the United Kingdom has, for instance, explicitly pointed out that ‘routine and legitimate information gathering’ does not constitute coercion, and thus is not prohibited intervention.¹⁰³ Instead, the most frequently used example of intervention in the cyber context given by states is the manipulation of elections by cyber means.

A related question is whether the disclosure of intelligence is a violation of the prohibition of intervention. Prior to Russia's renewed invasion in February 2022, Western states, and primarily the United States, released national intelligence to warn about Russian military plans and to build support for Ukraine.¹⁰⁴ Some international relations commentators view this form of public disclosure of intelligence as 'coercive'.¹⁰⁵ However, from a legal perspective such dissemination of sovereign intelligence does not constitute coercion, as the purloined information is not designed to compel Russia to change its behaviour. Instead, this form of public intelligence releases falls within the category of public diplomacy, persuasion, or propaganda, which is insufficient to qualify as coercion.¹⁰⁶

The non-intervention principle is generally considered a relatively narrow rule of international law. Therefore, a cyber operation must meet a considerably high threshold to constitute a prohibited intervention. Cyber espionage typically does not reach this threshold as it is not coercive vis-à-vis the *domaine réservé* of the target state.



Photo/Illustration and description: Mykola Mazuryk, Shutterstock.com
Binary code pattern in blue and yellow colors of flag of Ukraine.

CYBER AND INTELLIGENCE SUPPORT TO UKRAINE AND INTERNATIONAL LAW

In response to Russia's unlawful invasion of Ukraine, many Western states have supported the Ukrainian government with arms. This support primarily includes weapons, military equipment, and the training of Ukrainian soldiers to use different weapons systems. Some states – most notably the United States and Germany – have also shared military intelligence with Ukraine.¹⁰⁷ There are also reports that some states are assisting Ukraine's efforts to defend against Russian cyber warfare operations. Denmark has, for instance, publicly said that it is providing software to enable Ukraine's cyber defence.¹⁰⁸

Western states are engaged in a delicate balancing act. On the one side, they seek to support Ukraine in its survival struggle against Russia. On the other side, they avoid getting drawn into the conflict between Russia and Ukraine. Russia has, on several occasions, characterised the Western support as direct involvement in the conflict.¹⁰⁹ In a reaction to Denmark's and the Netherlands' decision to supply Ukraine with F-16 fighter jets, Russia proclaimed that this signified a 'growing involvement in the conflict surrounding Ukraine'.¹¹⁰ Yet, Western states have repeatedly rejected this interpretation and made it clear that they are not parties to the armed conflict.

The security assistance to Ukraine has not only raised political considerations about whether this support could cross so-called 'red lines' and risk further escalation of the conflict; the legal implications of such assistance have also been a key facet in the calculus regarding the support given.

The security assistance to Ukraine has not only raised political considerations about whether this support could cross so-called 'red lines' and risk further escalation of the conflict; the legal implications of such assistance have also been a key facet in the calculus regarding the support given.¹¹¹ States have, however, been rather reluctant to share their legal considerations openly.

When considering the legal consequences of providing intelligence and cyber assistance to Ukraine, three separate bodies of international law are particularly relevant: (1) the legality of the use of force by states (*ius ad bellum*), (2) the law of neutrality and (3) international humanitarian law (IHL), specifically the issue of co-belligerency.

Intelligence sharing and cyber support is lawful collective self-defence

A central question is whether sharing intelligence and cyber support breaches the prohibition on use of force in Article 2(4) of the UN Charter. If this is the case, the support constitutes an internationally wrongful act, and Russia could react with proportionate countermeasures.¹¹²

The threshold at which a cyber operation amounts to a use of force is still unsettled. However, there is widespread agreement that an operation that causes significant physical damage or injury crosses it. A state that conducts an offensive cyber

operation with destructive or injurious effects on Russian infrastructure would therefore likely breach the prohibition on the use of force.¹¹³ Similarly, a state that supports Ukraine with military intelligence that is used to conduct attacks against Russia would likely also amount to the use of force.¹¹⁴

But even if the sharing of intelligence and the cyber support rise to the level of the use of force, the assistance is a lawful defence of Ukraine. Ukraine undoubtedly enjoys a right to defend itself against the Russian invasion under the UN Charter Article 51 and under customary international law. Ukraine is also entitled to ask other states to act in collective self-defence against Russia. As a result, Ukraine can lawfully ask other states to assist with weapons, including cyber support and intelligence.¹¹⁵

Walking a fine line between neutrality and support

Another question is whether the support of intelligence and cyber means to Ukraine violates the law of neutrality. International neutrality law is an old body of law that seeks to regulate the legal relationship between those states that are engaged in an international armed conflict (belligerents), and those states that are not taking part (neutral states).¹¹⁶ Under the law of neutrality, a neutral state must not favour any of the belligerents militarily. Thus, neutral states must remain impartial towards the belligerent parties and refrain from providing war-related goods and services to either side of the conflict that could influence the outcome of the armed conflict.

Under a traditional conception of neutrality, providing intelligence to Ukraine could be considered a violation of the duty of impartiality.¹¹⁷ A state that shares so-called actionable military intelligence at the tactical level that enables Ukraine to either conduct military attacks against the enemy or to defend itself from adversarial attacks would undoubtedly violate the duty of impartiality.¹¹⁸ The same would likely also be the case when a state shares strategic-level intelligence with Ukraine about the overall political intentions of Russia.

In the same vein, a state that provides offensive cyberattack capabilities to Ukraine would also violate the duty of impartiality if aimed at Russian forces.¹¹⁹ Again, a state that is acting to support one belligerent in favour of the other breaches its neutrality obligation. The support of defensive cyber means would likely also violate the laws of neutrality, as such defensive measures could be considered 'war material of any kind' that contributes to Ukraine's general fighting capacity.¹²⁰

Some states, and most notably the United States, have adopted the doctrine of so-called 'qualified neutrality'. Under this approach a state that takes non-neutral acts in support of a victim of an unlawful aggression, in this case Ukraine, does not violate its duty of impartiality. From this perspective a state does not violate the law of neutrality by providing cyber means or intelligence to Ukraine.¹²¹ However, it is doubtful whether the qualified neutrality doctrine applies to Ukraine for the reason that the UN Security Council, which is the determiner of when there has been aggression, has not authorised military assistance to Ukraine.¹²² Moreover, Western states are not supporting Ukraine in response to a collective self-defence agreement, which could provide the necessary basis for assistance with qualified neutrality.¹²³

A state that violates its obligation of neutrality does not become a party to the conflict between Ukraine and Russia. However, Russia would be permitted to take nonforceful countermeasures within carefully proscribed legal limits against the state that supports Ukraine.


In sum, states that support Ukraine with intelligence and cyber support risk violating their obligation of neutrality under traditional conceptions of neutrality law. That being said, most states have likely already crossed that line by delivering heavy weapons and other types of military equipment to Ukraine. Thus, the practical implication of the support to Ukraine is more a matter of policy concerns over potential escalation risks and geographical spread of the war than one of legal line drawing.

Co-belligerency and the risk of becoming a part of the conflict

A separate legal question is whether a state becomes a party (a so-called 'co-belligerent') to the conflict with Russia by providing Ukraine with intelligence and cyber support. The answer to this question depends on whether this support directly harms Russia. Once a state becomes a party to an existing conflict, it loses its neutral status and becomes a co-belligerent under international humanitarian law.

There is widespread agreement among scholars that the supply of even heavy conventional weapons is insufficient to make a state a co-belligerent.¹²⁴ The reason is that only Ukrainian soldiers use these weapons against Russia. Conversely, intelligence support to Ukraine is more of a legal grey zone. Many scholars argue that a state supporting Ukraine with precision targeting intelligence such as geolocations that enable Ukrainian forces to target Russian military assets would

become a co-belligerent.¹²⁵ The provision of more strategic or broad operational intelligence on Russia's overall actions, capabilities and intentions is likely insufficient to make the state sharing the intelligence a party to the conflict.¹²⁶ The determining factor seems to be whether the shared intelligence is sufficiently granular to be used directly in the targeting process, i.e. Ukraine's planning and conduct of lethal attacks on Russian forces in real time.¹²⁷



The support of offensive cyber means that directly cause lethal or destructive harm to Russia could also make the assisting state a party to the conflict.

To avoid the risk of becoming a direct party to the conflict, states sharing intelligence with Ukraine have apparently chosen a pragmatic approach. For instance, Germany reportedly provides information on Russian troop movements to Ukraine, but with a delay of several days.¹²⁸ Other Western states carefully remove targeting information from intelligence that is provided to Ukraine to prevent it from enabling direct military strikes.¹²⁹

The support of offensive cyber means that directly cause lethal or destructive harm to Russia could also make the assisting state a party to the conflict.¹³⁰ By contrast, a state that provides Ukraine with cyber defence means cannot be seen to directly participate in the hostilities.

In sum, an assisting state may become a party to the conflict between Russia and Ukraine by providing actionable intelligence and offensive cyber means. Yet, due to the secret nature of cyber and intelligence support, it is difficult to determine whether any Western state has yet supported Ukraine in a manner that would qualify them as co-belligerents.




Photo/Illustration and description: Vektor Tradition, Shutterstock.com. Cyber spy technology, virtual eye of internet control surveillance and digital invigilation.

CONCLUSION

With the advent of the Internet, state-driven espionage has taken new forms. Digitalisation and the vast interconnectedness of networks have given states a wide geographical reach that allows them to collect, practically anonymously, large amounts of information without physical proximity to the target. Unsurprisingly, cyber espionage has become an attractive tool for states. This practice is likely to become even more common and widespread in an increasingly digitalised and connected world. State-sponsored cyber espionage is undeniably an integral part of what some scholars have conceptualised as an intelligence contest.

States participating in this intelligence contest in cyberspace are faced with an increasingly complex international legal landscape. Although it is universally accepted that international law applies to cyberspace, there is still much uncertainty on exactly how to interpret some of the most fundamental rules such as the principles of territorial sovereignty and non-intervention in the cyber context. As a result, states operating in cyberspace must carefully consider the potential legal implications of their activities.

States are also facing difficult strategic legal choices regarding their interpretation of international law in the cyber context. They must carefully balance the interests of operational freedom to conduct low-level cyber operations such as cyber espionage with the normative protection that well-defined rules give against the cyber operations of other states. It is not possible to have both.



In a conflict-ridden world, marked by strategic rivalry and distrust, states are undoubtedly reliant on intelligence to determine the capabilities and dispositions of other states.

This dilemma explains the more cautious and pragmatic approach that several Western states have taken with respect to their interpretations of the principles of sovereignty and non-intervention in the cyber context. For these states, remote-access cyber espionage neither breaches the principles of sovereignty nor those of non-intervention. By choosing this liberal interpretation of existing law, states have effectively determined that these fundamental principles should not restrict their state-sponsored cyber espionage activities.

This approach is not only legally desirable; it is also a matter of policy. Cyber espionage is a critical tool of statecraft that enables states to ensure national security and political and military power on the international level. In a conflict-ridden world, marked by strategic rivalry and distrust, states are undoubtedly reliant on intelligence to determine the capabilities and dispositions of other states. The insights gained through such activity can potentially lend stability to the international system as a whole as spying increases transparency about other states' intentions. From this perspective, states should avoid imposing legal limits on their mutual espionage activities through restrictive interpretations of international law, or through new international rules.

The Russia–Ukraine conflict has clearly illustrated how Western states have instrumentalised intelligence and assisted Ukraine with cyber support to change the outcome of the war in favour of Ukraine. This assistance has posed a multitude of legal challenges over how much and what type of aid states can give to a belligerent party within international law. The legality of this support must be assessed under various, different, legal regimes. Support to war-related intelligence or offensive cyber support qualifies as lawful collective self-defence under the UN Charter. However, states providing this support to Ukraine violate their duty of impartiality under traditional conceptions of neutrality. Similarly, states providing actionable battlefield intelligence or cyber support that directly support Ukraine’s military operations become parties to the ongoing conflict alongside Ukraine.

By way of conclusion, espionage has long been considered as taking place in the shadows of international law, as a ubiquitous phenomenon that exists in a legal black hole outside the scope of existing rules. States have traditionally been reticent to clarify whether, and if so how, existing international legal rules apply to their intelligence collection activities. But the advent of cyberspace has been a game changer and prompted states to shed some light on the legal implications of cyber espionage under international law. This development is important as it is states that play the primary role in the interpretation and making of international law.

NOTES

- 1 Julia Voo et al. (2020). 'National Cyber Power Index 2020', September 2020, 21.
- 2 For a comprehensive, but non-exhaustive, list of national statements see 'National Position', International Cyber Law: Interactive Toolkit, 20 March 2023.
- 3 Robert M. Chesney & Max W. E. Smeets (2023). *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*. Washington DC: Georgetown University Press.
- 4 Smeets & Chesney (2020).
- 5 Joshua Rovner (2019). 'Cyber war as an intelligence contest', *War on the Rocks*, <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/>
- 6 Smeets & Chesney (2020).
- 7 David P. Fidler (2021). 'SolarWinds and Microsoft Exchange: hacks wrapped in a cybersecurity dilemma inside a cyberspace crisis', *Georgetown Journal of International Affairs*, 12 April. <https://gjia.georgetown.edu/2021/04/12/solarwinds-and-microsoft-exchange-hacks-wrapped-in-a-cybersecurity-dilemma-inside-a-cyberspace-crisis/>
- 8 Danish Defence Intelligence Service (2022). 'Intelligence Outlook 2022', December 2022, 35.
- 9 Ministerie van Defensie (2023). 'Toespraak minister van Defensie bij MIVD-seminar Fog of War - Toespraak - Defensie.nl', toespraak. Ministerie van Defensie, 23 June. <https://www.defensie.nl/downloads/toespraken/2022/06/23/toespraak-minister-mivd-seminar-fog-of-war>. (Text translated using Google Translate).
- 10 Ofek Riemer & Daniel Sobelman (2023). 'Coercive disclosure: the weaponization of public intelligence revelation in international relations', *Contemporary Security Policy* 44(2): 276–307.
- 11 Tim Maurer (2020). 'A dose of realism: the contestation and politics of cyber norms', *Hague Journal on the Rule of Law* 12(2): 283–305, <https://doi.org/10.1007/s40803-019-00129-8>.
- 12 National Intelligence Council (2021). *Global Trends 2040 A More Contested World* (Washington DC: National Intelligence Council): 103.
- 13 Michael N. Schmitt (2020a). 'Taming the lawless void: tracking the evolution of international law rules for cyberspace', *Texas National Security Review* 3(32–47): 37–38.
- 14 Michael Schmitt (2022a). 'The law of cyber conflict: quo vadis', *Articles of War*, Lieber Institute, West Point (blog), 22 July, <https://lieber.westpoint.edu/law-cyber-conflict-quo-vadis/>
- 15 Kevin Jon Heller (2021). 'In Defense of pure sovereignty in cyberspace', *International Law Studies*, 97: 1493.
- 16 Schmitt (2020a).
- 17 Schmitt (2022a).
- 18 Duncan B. Hollis & Barrie Sander (Forthcoming 2023). 'International law and cyberspace: what does state silence say?' In: *State Silence Across International Law* (OUP).
- 19 Dan Jerker B. Svantesson et al. (2021). *The Developing Concept of Sovereignty: Considerations for Defence Operations in Cyberspace and Outer Space* (Bond University: Technology and Jurisdiction Legal Research Team), p. 41.
- 20 Michael Schmitt, ed. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second edition, Cambridge University Press, p. 169.

- 21 Svantesson et al. (2021), p.41.
- 22 Paul C. Ney, Jr. (2020). 'DOD General Counsel Remarks at US Cyber Command Legal Conference', 2 March.
- 23 Ney, Jr. (2020).
- 24 See footnote 16 in Government of Canada, 'International Law Applicable in Cyberspace' (Government of Canada, April 2022).
- 25 See footnote 2 in Ministry of Defence of France, 'International Law Applied to Operations in Cyberspace', 9 September 2019.
- 26 See footnote 6 in 'Norwegian positions on selected questions of international law relating to cyberspace', May 2021.
- 27 Suella Braverman (2022). 'Speech: International Law in Future Frontiers', 19 May, <https://www.gov.uk/government/speeches/international-law-in-future-frontiers>
- 28 'International law in future frontiers - Meeting Transcript', Royal Institute of International Affairs, 19 May 2022, p. 17.
- 29 Ministry of Foreign Affairs of Costa Rica, 'Costa Rica's position on the application of international law in cyberspace', 21 July 2023, p. 6.
- 30 Naomi Hart (2022). 'Espionage and elusive rules of customary international law'. In The Oxford Process on International Law Protections in Cyberspace: A Compendium. Oxford Institute for Ethics, Law and Armed Conflict, p. 300.
- 31 'UNASUR's draft statement on 'Other Disarmament Measures and International Security', October 2016.
- 32 Russell Buchan, "Cyber espionage, international law and the protection of digital supply chains", i The Oxford Process on International Law Protections in Cyberspace: A Compendium (Oxford Institute for Ethics, Law and Armed Conflict, 2022), 334.
- 33 Hart (2022), p. 300.
- 34 See e.g. 'AVID Annual Report 2019'. General Intelligence and Security Service of the Netherlands. April 2020, p. 7.
- 35 'Fact Sheet: President Xi Jinping's State Visit to the United States', 25 September 2015. <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>
- 36 'Fact Sheet: President Xi Jinping's State Visit to the United States' (2015).
- 37 'Joint Communiqué – 2nd Canada–China High-Level National Security and Rule of Law Dialogue', Prime Minister of Canada, 22 June 2017, <https://rb.gy/3h6kh>
- 38 Information and Communications Technology (ICT).
- 39 Ministry of Foreign Affairs of Japan (2016). 'G7 Principles and Actions on Cyber'. 27 May 2016. <https://www.mofa.go.jp/files/000160279.pdf>
- 40 Forsvarsdepartementet (2018) 'Høringsnotat – Forslag til ny lov om Etterretningstjenesten' 12 November, p. 143.
- 41 Braverman (2022).
- 42 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States'. Attached to the 2021 UN GGE Report (UNODA, August 2021), p. 18, https://ccdcoe.org/uploads/2018/10/UN-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf
- 43 Government of Canada, International Law applicable in cyberspace, April 2022.

- 44 Ministry of Foreign Affairs of the People's Republic of China (2021). 'China's Views on the Application of the Principle of Sovereignty in Cyberspace', p. 3.
- 45 Government of Canada, International Law applicable in cyberspace, April 2022, p. 6, para 19.
- 46 Richard Kadlčák (2020). 'Statement of the Special Envoy for Cyberspace and Director of Cybersecurity Department of the Czech Republic', 11 February.
- 47 Government of Denmark (2023). 'Denmark's position paper on the application of international law in cyberspace: Introduction', *Nordic Journal of International Law* 4(2-4). <https://doi.org/10.1163/15718107-20230001>
- 48 'International law and cyberspace. Finland's national position' (2020) Ministry for Foreign Affairs.
- 49 Ministry of Defense of France, 'International Law Applied to Operations in Cyberspace'. 9 September 2019
- 50 The Federal Government of Germany (2021). 'On the Application of International Law in Cyberspace (Position Paper)'. The Federal Government of Germany, March 2021.
- 51 'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace'. August 2020.
- 52 Irish Department of Foreign Affairs (2023). 'International Law and Cyberspace', 6 July 2023.
- 53 'Italian position paper on International law and cyberspace' (Italian Ministry for Foreign Affairs and International Cooperation)
- 54 'Basic Position of the Government of Japan on International Law Applicable to Cyber Operations' (2021) Ministry of Foreign Affairs of Japan, 28 May 2021.
- 55 'Government of the Kingdom of the Netherlands, Appendix: International law in cyberspace'. 26 September 2019.
- 56 New Zealand Foreign Affairs & Trade (2020). 'The application of international law to state activity in cyberspace', p. 1. December 2020.
- 57 Norway's Position Paper on International Law and Cyberspace' (2023) 92(3) *Nordic Journal of International Law*.
- 58 'The Republic of Poland's position on the application of international law in cyberspace' (2022) Ministry of Foreign Affairs of Poland, 29 December 2022.
- 59 'Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by states'. Attached to the 2021 UN GGE Report', p. 76.
- 60 'Position Paper on the Application of International Law in Cyberspace' (2022) Government Offices of Sweden. July 2022.
- 61 'Switzerland's position paper on the application of international law in cyberspace' (2021) Federal Department of Foreign Affairs, May 2021, Annex UN GGE 2019/2021
- 62 'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace', 2020.
- 63 Ministry of Defense of France, 'International Law Applied to Operations in Cyberspace'. 9 September 2019, pp. 10-11.
- 64 Heller (2021); Russell Buchan (2018). *Cyber Espionage and International Law*. Hart Publishing.
- 65 Government of Canada, International Law applicable in cyberspace, April 2022.

- 66 Kadlčák (2020).
- 67 Government of Denmark (2023): 'Introduction', pp. 2–4.
- 68 'International law and cyberspace. Finland's national position'.
- 69 See e.g. Government of Denmark (2023): Introduction, p. 4; 'Norwegian positions on selected questions of international law relating to cyberspace', p. 4.
- 70 See e.g., 'Norwegian positions on selected questions of international law relating to cyberspace'; Government of Denmark (2023): Introduction; 'Switzerland's position paper on the application of international law in cyberspace' (2021).
- 71 Schmitt (2017). pp. 21–22.
- 72 International law applicable in cyberspace, Government of Canada, April 2022, para 10.
- 73 New Zealand Foreign Affairs & Trade (2020), para 14.
- 74 Ney, Jr. (2020).
- 75 'China's Views on the Application of the Principle of Sovereignty in Cyberspace', p. 2.
- 76 Ibid.
- 77 'Annual Threat Assessment of the US Intelligence Community'. Office of the Director of National Intelligence. 7 February 2022, p. 8; 'Switzerland's security 2020, Situation Report of the Federal Intelligence Service' (2020), p. 76.
- 78 Joe Devanny & Buchan Russell (2023). 'Brazil's cyber strategy under Lula: not a priority, but progress is possible', Carnegie Endowment for International Peace, pp. 14–16. <https://carnegieendowment.org/2023/08/08/brazil-s-cyber-strategy-under-lula-not-priority-but-progress-is-possible-pub-90339>
- 79 'Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of information and communications technologies by States'. Attached to the 2021 UN GGE Report', p. 18.
- 80 'Costa Rica's position on the application of international law in cyberspace', p. 7.
- 81 Duncan B. Hollis & Chris Carpenter, 'A victim's perspective on international law in cyberspace', 28 August 2023. <https://www.lawfaremedia.org/article/a-victim-s-perspective-on-international-law-in-cyberspace>
- 82 'Putin: cyber espionage is direct violation of state's sovereignty', Russia & CIS General Newswire, 11 July 2014.
- 83 For an analysis of Russia's understanding of sovereignty in cyberspace see Asbjørn Thranov and Flemming Splidsboel Hansen (2021). 'Trying to govern the ungovernable'. DIIS Policy Brief. <https://www.diis.dk/en/research/trying-to-govern-the-ungovernable>
- 84 Michael Schmitt (2020b). 'Top expert backgrounder: Russia's SolarWinds operation and international law', Just Security (blog), 21 December 2020.
- 85 'The Republic of Poland's position on the application of international law in cyberspace' (2022), p. 3.
- 86 Joshua Rovner (2020) 'The Intelligence Contest in Cyberspace', Lawfare (blog), 25 March 2020.
- 87 UN GGE (2021). 'Group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security', 14 July 2021.
- 88 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment (Merits) [1986] ICJ Rep. 14. para. 205.

- 89 Katja S. Ziegler (2013). 'Domaine Réservé'. In: Max Planck Encyclopedia of Public International Law [MPEPIL].
- 90 Gary P. Corn (2022) 'Covert deception, strategic fraud, and the rule of prohibited intervention'. In: The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment. New York: Oxford University Press, p. 214.
- 91 Schmitt (2020b).
- 92 Michael Schmitt, Top Expert Background: Russia's SolarWinds Operation and International Law' (21 December 2020) <<https://www.justsecurity.org/73946/russias-solarwindsoperation-and-international-law>>
- 93 UN GGE (2021), p. 19.
- 94 Government of Denmark (2023): Introduction, p. 5.
- 95 'Italian position paper on International law and cyberspace', pp. 4–6.
- 96 Government of the Kingdom of the Netherlands (2019) Appendix: International law in cyberspace', p. 3.
- 97 Australian Government (2020). 'Australia's position on how international law applies to State conduct in cyberspace'.
- 98 New Zealand Foreign Affairs & Trade (2020).
- 99 Braverman (2022).
- 100 Caroline Krass (2023). 'Implementing integrated deterrence in the cyber domain: the role of lawyers', Lieber Institute, West Point. 18 April 2023. <https://lieber.westpoint.edu/implementing-integrated-deterrence-cyber-domain-role-lawyers/>
- 101 New Zealand Foreign Affairs & Trade (2020), p. 2.
- 102 Krass (2023).
- 103 Braverman (2022).
- 104 Warren P. Strobel (2022). 'Release of Ukraine intelligence represents new front in US information war with Russia', Wall Street Journal, 4 April 2022.
- 105 Riemer & Sobelman (2023).
- 106 Schmitt (2017) p. 318. See also Government of Denmark (2023). Introduction, p. 5.
- 107 dpa-AFX International ProFeed (2022). 'Report: German intelligence supporting Ukraine with information', 28 September 2022; Strobel (2022).
- 108 Forsvarsministeriet (2023). 'Faktaark: Millitære donationer og støtte for knap 5 mia. kr. til Ukraine'. http://www.fmn.dk/globalassets/fmn/dokumenter/nyheder/2023/-2023-faktaark_stoette-til-ukraine-w-.pdf
- 109 AP News (2022). 'Russian FM: US, NATO Directly Involved in Ukraine Conflict', 1 December 2022. <https://apnews.com/article/russia-ukraine-nato-europe-business-moscow-5b3ca7ea4e005c0908fb86b6d28f79d5>
- 110 The Ministry of Foreign Affairs of the Russian Federation' (2023) 'Foreign Ministry Spokeswoman Maria Zakharova's comment on the Ukrainian crisis'. Accessed 30/8/23. https://mid.ru/en/foreign_policy/news/1901692/
- 111 See e.g. Wissenschaftliche Dienste des Deutschen Bundestages (2022). 'Rechtsfragen der militärischen Unterstützung der Ukraine durch NATO-Staaten zwischen Neutralität und Konfliktteilnahme', March 2022; Congressional Research Service (2022). 'Legal sidebar: international neutrality law and US military assistance to Ukraine', 26 April 2022.

- 112 Kevin Jon Heller & Lena Trabucco (2022). 'The legality of weapons transfers to Ukraine under international law', *Journal of International Humanitarian Legal Studies* 13(2): 254. <https://doi.org/10.1163/18781527-bja10053>
- 113 Michael N. Schmitt (2022b) 'Ukraine Symposium – US Offensive Cyber Operations in Support of Ukraine', Lieber Institute West Point, 6 June 2022, <https://lieber.westpoint.edu/us-offensive-cyber-operations-support-ukraine/>
- 114 Michael N. Schmitt (2022c), 'Ukraine Symposium – Are we at War?', *Articles of War*, Lieber Institute, 9 May 2022, <https://lieber.westpoint.edu/are-we-at-war/>
- 115 Heller & Trabucco (2022), pp. 254–55; Schmitt (2022c).
- 116 Neutrality law is codified in Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (1907) and Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War (1907).
- 117 Schmitt (2022c); Heller & Trabucco (2022), p. 257.
- 118 Heller & Trabucco (2022), p. 257.
- 119 Schmitt (2022b).
- 120 See Hague Convention XIII art. 6 ('The supply, in any manner, directly or indirectly, by a neutral Power to a belligerent Power, of warships, ammunition, or war material of any kind whatever, is forbidden.')
- 121 Schmitt (2022b).
- 122 Heller & Trabucco (2022), p. 262.
- 123 Michael N. Schmitt (2023). 'Providing Arms and Materiel to Ukraine: Neutrality, Co-Belligerency, and the Use of Force', Lieber Institute West Point, 30 August 2023, <https://lieber.westpoint.edu/ukraine-neutrality-co-belligerency-use-of-force/>
- 124 Heller & Trabucco (2022), p. 265; Alexander Wentker (2023). 'At war? Party status and the war in Ukraine. *Leiden Journal of International Law*, 36(3), 643–656. doi:10.1017/S0922156522000760
- 125 Heller & Trabucco (2022), p. 264; Wentker, 'At War? Party Status and the War in Ukraine'; Schmitt (2022b).
- 126 Schmitt (2022b).
- 127 Militärische Unterstützung der Ukraine: Wann wird ein Staat zur Konfliktpartei? Wissenschaftlichen Dienste des Deutschen Bundestages – WD2 -3000 – 023/23, 15.
- 128 Die Zeit. Thai News Service (2022). 'Germany/Ukraine: Germany's BND shares intelligence with Kiev'. 30 September 2022.
- 129 'West careful about sharing intelligence with Ukraine', i-Independent Print Ltd. 9 March 2022.
- 130 Wentker (2023), p. 12; Schmitt (2022b).

DIIS · Danish Institute for International Studies

The Danish Institute for International Studies is a leading public institute for independent research and analysis of international affairs. We conduct and communicate multidisciplinary research on globalisation, security, development and foreign policy. DIIS aims to use our research results to influence the agenda in research, policy and public debate, and we put great effort into informing policymakers and the public of our results and their possible applications.

Defence and Security Studies at DIIS

This publication is part of the Defence and Security Studies at DIIS. The aim of these studies is to provide multidisciplinary in-depth knowledge on topics that are central for Danish defence and security policy, both current and long-term. The design and the conclusions of the research under the Defence and Security Studies are entirely independent. All reports are peer-reviewed. Conclusions do not reflect the views of the ministries or any other government agency involved, nor do they constitute an official DIIS position. Additional information about DIIS and our Defence and Security Studies can be found at www.diis.dk.

Subscribe to DIIS's Newsletter





DIIS · DANISH INSTITUTE FOR INTERNATIONAL STUDIES

Gl. Kalkbrænderi Vej 51A | DK-2100 Copenhagen | Denmark | www.diis.dk