Sovereignty in Cyberspace: Lessons from the Ukrainian Case

Pijpers, P.; Pouw, E.

Publication date
2022
Document Version
Final published version
Published in
Atlantisch Perspektief

Sovereignty in Cyberspace: Lessons from the Ukrainian Case

Peter Pijpers and Eric Pouw

Since the annexation of the Crimean Peninsula in 2014, tension has risen between Ukraine and the Russian Federation. Numerous small incidents, conflicts or intrusions in cyberspace followed, including in the prelude to the 2022 Ukraine-Russia war. Individually, none of these reached the threshold of the use of force or an armed attack. It was only after the actual invasion that the wider international community responded - unfortunately, since the international community could have responded earlier when sovereignty or the principle of non-intervention was violated. What can we learn from this for future conflicts?

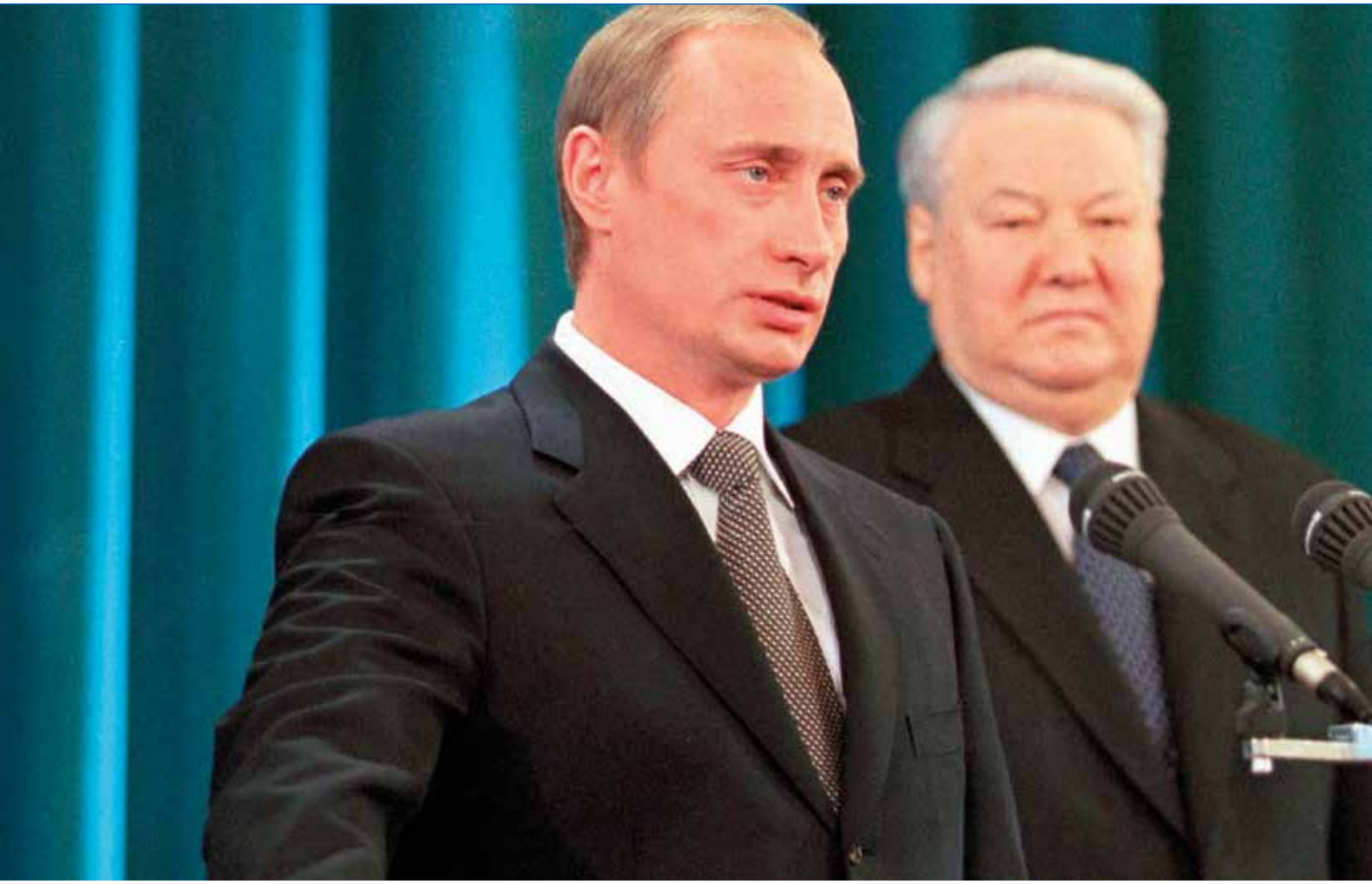
In hindsight, the invasion of Ukraine by the Russian Federation (RF) might have been logical and inevitable. Since the dismantling of the Soviet Union, the RF has been struggling with its new identity. Was it to become a liberal democracy amalgamated in the Western world or should it redefine its own identity as the Greater Russia, viewing the Western world, and NATO in particular, as a threat? With the emergence of Vladimir Putin on the political stage, some 20 years ago, the latter appeared to be the way ahead.

With the renaissance of the notion of Greater Russia, one of the objectives of the RF is to obtain strategic depth, a buffer zone or a sphere of influence around RF's (physical and virtual) boundaries, which explains the close Sino-Russian bond and current affiliation with the Belarus regime. Ukraine was also expected to fall into line, but it did not.

The RF has been influencing Ukrainian politics ever since the Orange revolution in 2004. Tension peaked when RF annexed Crimea in 2014 after which pro-Russian separatists seized the opportunity to gain influence and power in the eastern provinces of Donetsk and Luhansk – areas with a large Russian minority. The tensions culminated in the Maidan protests in 2014. During these protests it became clear that Ukraine was leaning towards a liberal democracy rather than the RF's way of governance. Ukraine expressed its wish to join the EU and NATO, which would be detrimental for the RF objective of creating strategic depth.

The persistent RF infringements, provocations and undermining activities, especially via cyberspace, have increased since the Maidan protests and include the 2015 and 2016 "BlackEnergy" cyberattacks, resulting in an electricity outage in large parts of Ukraine.

The attacks in or via cyberspace did not wane after the so-called special military operation on February 24, 2022. Outraged by this unlawful armed attack on Ukraine, which amounts to violation of the prohibition on the use of force as set forth in Article 2(4) UN Charter, States have taken numerous political, economic and legal measures to force the RF to cease its operations. Viewed from an international-law perspective, the question is, however: could the international community have reacted prior to this attack? If so, how? And why did they refrain from doing so?



Since the dismantling of the Soviet Union, the Russian Federation has been struggling with the question whether it should become a liberal democracy or whether it should redefine its own identity as the Greater Russia. With the emergence of Vladimir Putin on the political stage the latter appeared to be the way ahead. Pictured is Putin taking his presidential oath in May 2000 (photo: Wikimedia Commons / Kremlin.ru)

THE FOREIGN CYBER CAMPAIGN IN THE UKRAINE

The Russia-Ukraine war started on February 24, 2022, but Ukraine has been under attack much longer.[1] Maybe not always in a traditional kinetic way, but most certainly via cyberspace. Government websites were hit by DDoS attacks, temporarily taking them down,[2] or defaced by a malicious cyber group called UNC1151.[3] Furthermore, Whisper Gate malware was placed on the ICT infrastructure of government agencies providing emergency response functions, which might have destroyed files rendering the systems they work on inoperable.[4] These cyber operations were directed at cyberspace itself. Apart from these digital sabotage operations, digital influence operations were witnessed, such as the leaking of personal data, using cyberspace as a vector to target the cognitive dimension of adversaries.[5]

Whilst many of these cyber-related attacks cannot definitively be attributed to a State or non-State actor, it can be assumed that this campaign – which can entail several operations - most likely originates from outside Ukraine, and will not reach the threshold of the threat or use of force (under the terms of Article 2(4) of the UN Charter), let alone amount to an armed attack (under the terms of Article 51 UN Charter).

The absence of force does not imply that international law simply permits these below-the-use-of-force cyber campaigns. An intrusion into the ICT system of another State to manipulate election results will not amount to the use of force but can still result in a violation of international law.

Below the use of force, the legal standards of sovereignty and non-intervention regulate the behavior between States. The application of these standards to cyberspace is, however, contested due to diverging interpretations, and because not all cyber operations (below the threshold of the use of force) are unlawful per se. Using propaganda to persuade foreign audiences or political leaders might be unwelcome, but it is not unlawful. Conversely, campaigns compelling the target audience to comply with the will of the attacker are coercive and, in general, unlawful. Most cyber campaigns by foreign actors are, however, neither persuasive nor compelling, but manipulative and deceitful by nature, as is the case in Ukraine.

The next two sections will assess when the (manipulative) cyber campaign against Ukraine violates the international law standards of sovereignty and non-intervention, thereby focusing on the prelude to the war – prior to February 24, 2022.

THE CYBER CAMPAIGN AS A BREACH OF SOVEREIGNTY

Though sovereignty is not the most transparent legal notion in definition or in status, Arbiter Huber provided a comprehensive description in the 1928 Island of Palmas Case: 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[6] Based on this definition sovereignty can be – for analytical purposes - divided into territorial integrity and political independence.

Territorial Integrity

Territorial integrity relates to the control over access and egress from the territory. A violation of territorial integrity is an act that is invasive of the territory of a State, the territorial sea or the airspace above it. Territorial integrity can be violated in numerous ways, physically or virtually.

Related to Ukraine, should foreign (special forces or intelligence) operators of State A access Ukraine and launch

> *Territorial integrity is more difficult to align with the virtual dimension of cyberspace*

cyber operations from Ukraine without the latter's consent, then State A violates the territorial integrity, and hence the sovereignty of Ukraine. However, unlike physical activities, cyber operations – including those mentioned above - hardly ever physically cross borders and are most often executed remotely from outside the target State.

The so-called Tallinn Manual sets out when a breach of territorial integrity of a State takes place as a result of a remotely executed cyber campaign.[7] The first threshold is that the cyber operation must have an effect causing physical damage, such as the destruction of a computer or a radar installation. A second – less severe – threshold is reached when the remote cyber operation causes a permanent functional impairment to the hard- or software. The impairment is permanent if software needs to be reinstalled, such as after the Shamoon malware incident,[8] but also defacing a website or deleting data could fall under this category. Damage below functional impairment (the third category) could be the slowing down of the processor of a computer, a DDoS-attack or temporary blackout.

While physical damage is reasonably undisputed, the other categories are more difficult to substantiate as violations of territorial integrity particularly since cyberspace can only partially be connected to the territory of a State based on the physical network layer of computers and routers. Activities that harm or damage the physical network layer, such as the destruction of computers, will breach territorial integrity and thus the sovereignty of the injured State.

Territorial integrity is more difficult to align with the virtual dimension of cyberspace: software, data and virtual persona (email addresses, Twitter accounts). Nonetheless, malign remote computer intrusion (hack) can still breach territorial integrity if data are deleted or altered. This would be the case when malware is installed to gather data and channel it to another computer, thereby undermining the integrity of the virtual dimension.

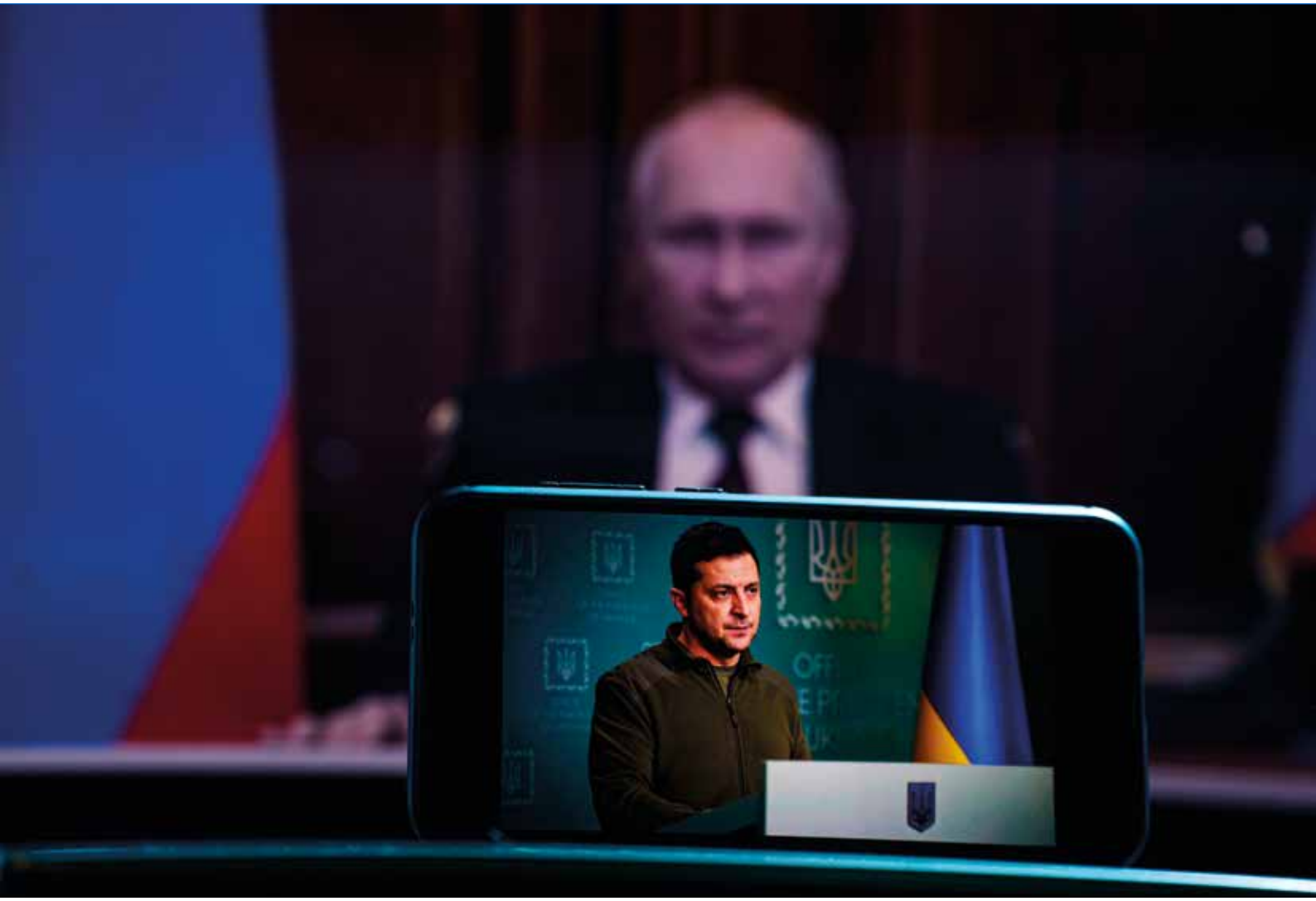
Apart from physical and virtual effects, remotely executed manipulative influence operations (using cyberspace as a vector to disseminate disinformation or leak sensitive data) affect the cognitive dimension and are not likely to violate the territorial integrity in a direct way. Nonetheless, indirect violations could affect territoriality, if the influence operation incites groups to revolt against the government.

Taking the Ukrainian case, territorial integrity will be breached if foreign operators are in Ukraine, without Ukrainian consent, conducting malign cyber campaigns. Digital sabotage (hacking) operations could breach territorial integrity if they cause functional damage as a result of defacements or result in impairments below functional damage due to the emplacement of malware on Ukrainian ICT infrastructure or the wiping of data – which were witnessed. Digital influence operations will not easily breach territorial integrity.

Political Independence

Despite the assessment that territorial integrity is difficult to align with remotely executed cyber campaigns, sovereignty can still be violated if the operations within the cyber campaign breach political independence.

The functions of the State form, as Huber mentioned, the core of political independence. These 'inherently governmental functions' are intimately related to the public in-



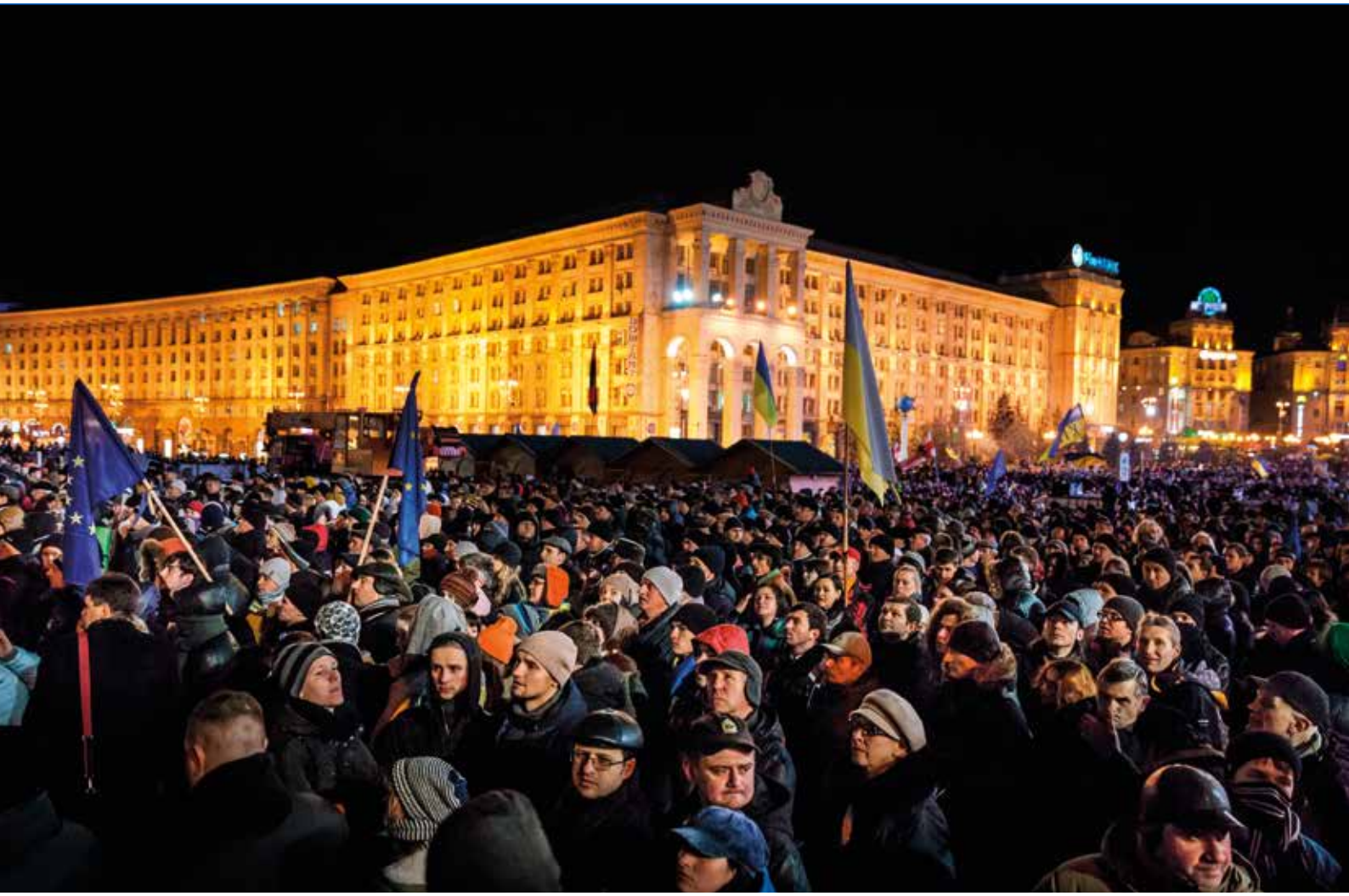
The Russia-Ukraine war started on February 24th, 2022. However, Ukraine has been under attack much longer, not always in the usual kinetic way but most certainly through cyberspace. Government websites were hit by DDos attacks or defaced by a malicious cyber group called UNC115. Pictured are the presidents of Russia and Ukraine (photo: Rokas Tenys / Shutterstock.com)

terest. State functions are universal and include national defense, tax collection, law enforcement and conducting elections, but exclude purely commercial activities. An infringement of State functions impairs the State's ability to perform these functions as it wishes. This threshold is crossed when State A is taking over (usurping) the State functions of State B and conducting them without the latter's consent, for example by taking over the electronic counting of votes after an election. State A similarly infringes the inherently governmental functions of State B by interfering with or disturbing them. Infringement of State functions amounts to a violation of political independence.[9]

Political independence is not affected when applied in cyberspace, in contrast to the notion of territorial integrity. Though political independence has a territorial link, a breach of political independence is not related to the persons and materiel on territory but to the activities (or functions) of the State.

Regarding the ongoing cyber campaign against Ukraine, targeting government websites could be an infringement of State functions of Ukraine if these websites are meant for dissemination of public information e.g. related to crisis-management functions. So far, there have been no reports that State functions were taken over, but it is possible that there was a disturbance or interruption, which would amount to an interference with, hence breach of, political independence - if attributable to a State actor.

Based on the above, there are indicators that both territorial integrity and political independence were or could have been breached as a result of the cyber campaigns against Ukraine. Though more data are required on the actual course of event and to attribute the cyber operations to a State actor, these are not the only impediments to invoking countermeasures. Not all States agree that sovereignty is a primary rule of international law in cyberspace; some argue it is not more than a principle of law.[10] Following that interpretation, the ongoing cyber operations are not unlawful. Hence, there is no legal ba-



The persistent Russian infringements, provocations and undermining activities against Ukraine, especially via cyberspace, have increased since the Maidan protests of 2013 (pictured) (photo: Drop of Light / Shutterstock.com)

sis to take countermeasures and any countermeasures taken would themselves be unlawful. Moreover, the legal interpretations of those States that do consider sovereignty a primary rule of law diverge. For example, while France and Switzerland argue that all incursions into the ICT infrastructure violate sovereignty, which also means that cyber espionage is unlawful,[11] others – including the Netherlands, Canada and Germany - argue that negligible effects below a certain threshold will not constitute a violation of sovereignty.[12] Though States must be applauded for expressing their legal opinion - decreasing the number of States staying on the fence – their diverging opinions increase legal uncertainty.

THE CYBER CAMPAIGN AS A VIOLATION OF THE PROHIBITION OF INTERVENTION

State sovereignty entails territorial integrity and political independence. A corollary of State sovereignty is the prohibition to intervene in another State. An intervention is a coercive incursion in the reserved domain of another state – the domain exclusive to the State, in other words not governed by treaties or customary international law.[13] Everything within this reserved domain, including private sectors, belongs to the jurisdiction of the State. As noted, a fundamental rule in international law is the prohibition to intervene in the affairs of another State,[14] i.e. to coercively intrude in those affairs.

Coercion is the essential element of an intervention.[15] Coercion is not a legal term, but it does have legal consequences. Based on the writings of legal scholars, coercion comprises three elements. The coercive intervention must a) undermine the control and autonomous decision-making process of the target State, b) in an intentional and deliberate way, c) with the aim to change the policies of that State. A coercive intervention does not need to succeed; a failed attempt still is coercive.

The cyber campaign against Ukraine targets its reserved domain, i.e. matters in which each State is permitted to decide freely. However, acts such as the leaking of personal data are disturbing and manipulative, but these are not coercive. Whilst the cyber campaign is not coincidental, it is more difficult to assess whether current activities are able to undermine the control of the government of

Ukraine, or what the purpose of the campaign is. Unfortunately, it becomes increasingly challenging to establish a case of coercion in cyberspace. Not only have the number and range of actors in cyberspace increased; the attributes of cyberspace have also been conducive to a variety of ways in which the actors can engage with (other) States in a stealthy fashion. Consequently, the risk is that, in cyberspace, only the most severe forms of coercion – those resembling the use of force - would amount to an intervention.

THE REMAINING LEGAL UNCERTAINTY

Despite the absence of force in the prelude to the war in Ukraine, the cyber campaigns could have amounted to breaches of international law based on the standards of sovereignty and the prohibition of intervention. The question that remains is why Ukraine or the wider international community did not respond to the potential breaches.

On the one hand, the response inadvertently reflects the (legal) uncertainty. If a breach of international law cannot be attributed to a State, invoking an internationally wrongful act and thus resort to countermeasures are difficult. Moreover, if the community of States has no shared view on the interpretation of the rules of international law, including on whether or not sovereignty is a primary rule of law in cyberspace, it will be even more challenging to determine how to respond to malign cyber campaigns. Finally, when States do provide their legal opinions on how international law applies to cyberspace, we have come to realize that their interpretations diverge, which only further increases the legal uncertainty within international law.

On the other hand, States might be deliberately reticent to respond since the legal uncertainty could suit them. The legal uncertainty allows States to 'cherry-pick'[16] from international law in such a way that it serves their national interests, cognizant that other States will not respond due to self-imposed restrictions.

Of course, with the military intervention in Ukraine on February 24 the RF has flagrantly breached international law and *ipso facto* the sovereignty of Ukraine. Though a discourse on the breach of sovereignty or non-intervention alone is rather academic during a war, the RF is still violating the political independence of Ukraine and intervenes in Ukraine's State functions especially in the Donbas area.

What we can learn for future operations is that it is possible to respond to inter-State cyberattacks before the actual armed conflict takes place, even if these attacks are below the threshold of the use of force. But, the decision to act is a political one which will reflect the State's own legal opinion regarding the application of international law in cyberspace, and its subsequent State behavior.

The situation in Ukraine reveals that the standards of international law can prove challenging when applied to operations in cyberspace, but above all that States eclectically use international law to further their interests. This results in unwelcome legal uncertainty subsequently hampering responses and undermining stability.

Peter Pijpers PhD, is Associate Professor of Cyber Operations at the Netherlands Defense Academy (NLDA) and researcher at the University of Amsterdam (UvA).

Eric Pouw PhD, is a senior legal advisor with the Netherlands Royal Army, and researcher at the Amsterdam Centre for International Law (UvA)

Would you like to react?
Mail the editor: redactie@atlcom.nl.

1. Federico Berger, "Ukraine's Government under Massive Cyberattack," *NDC Foundation*, 2022.
2. Stephanie Pell, "Contextualizing Last Week's Malicious Cyber Activities Against Ukrainian Government Websites and Systems," *Lawfare*, 2022.
3. Pavel Polityuk, "Ukraine Suspects Group Linked to Belarus Intelligence over Cyberattack," *Reuters*, January 16, 2022.
4. Tom Burt, "Malware Attacks Targeting Ukraine Government," *Microsoft* January (2022).
5. Peter B.M.J. Pijpers and Kraesten L. Arnold, "Conquering the Invisible Battleground," *Atlantisch Perspectief* 44, no. 4 (2020).
6. PCA, Island of Palmas Case (The Netherlands v United States), II Reports of International Arbitral Awards 829–71 (1928).
7. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017).
8. Nicole Perlroth and Clifford Krauss, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *The New York Times,* 2018.
9. Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (2018).
10. Jeremy Wright, "Cyber and International Law in the 21st Century," 2018.
11. Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace," 2019.; Swiss Federal Department of of Foreign Affairs, "Switzerland's Position Paper on the Application of International Law in Cyberspace - Annex UN GGE 2019/2021," 2021.
12. Ministry of Foreign Affairs, "Letter to the President of the House of Representatives on the International Legal Order in Cyberspace - Appendix : International Law in Cyberspace" (2019).; German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace," 2021.
13. PCIJ, Nationality Decrees in Tunis and Morocco - Advisory Opinion, Series B PCIJ Reports (1923).
14. See also the language used in Article 2(7) UN Charter related to UN institutions: "Nothing (…) shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state (…)".
15. Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986).
16. Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law," *Texas National Security Review* 3, no. 3 (2020).