Hybrid CoE Paper 15

Exploiting cyberspace: International legal challenges and the new tropes, techniques and tactics in the Russo-Ukraine War

Hybrid CoE

Peter B.M.J. Pijpers – October 2022

Hybrid CoE Papers are finalized pieces of analysis on a topic related to hybrid threats, based on one or several research questions. They may be either conceptual analyses or based on a concrete case study with empirical data.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN (web) 978–952–7472–48–4
ISBN (print) 978–952–7472–49–1
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

October 2022

Cover photo: enzozo / shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

Summary

The Russian invasion of Ukraine, while primarily a kinetic war, saw new actors and novel activities exploiting cyberspace. Numerous non-state actors, hacker groups and commercial enterprises have entered the virtual battlespace, taking sides with one of the warring states without necessarily being belligerent entities. While states were already struggling with how to regulate activities in cyberspace, the new tropes, techniques and tactics have increased legal uncertainty. International law is based on the state, a territory, and the distinction between war and peace, while cyberspace and the activities conducted therein are not. The Russo-Ukraine war has made it clear that non-state actors such as Microsoft or Anonymous cannot be attributed to a state, and that they do not participate directly in hostilities, at least not physically. Moreover, the attributes of cyberspace have not only blurred the differences between state and non-state actors, but also transformed the dichotomy between war and peace. Not only do the challenges of how to apply international law to the new tropes, techniques and tactics in cyberspace increase differences in interpretation, but the ensuing uncertainties can be exploited, causing legal asymmetry.

Introduction

Cyberspace simultaneously poses both opportunities and challenges. Commerce and communication benefit from the low cost of entry, the speed and reach of the domain, and the ability to penetrate the capillaries of society. But cyberspace can equally empower malign actors willing and able to exploit it, and can likewise enable conflict.

Existing malign activities that are now being undertaken in cyberspace include cyber-espionage, cyber-crime, subversion[1] or foreign election interference.[2] But function does not only follow form, as cyberspace has also enabled previously unheard-of malign activities such as wiper malware, distributed denial-of-service (DDoS) attacks or ransomware.[3] With the emergence of cyberspace, data and information is no longer solely a tool for gaining intelligence, insight and foresight in order to expedite decisions. Cyber-enabled information and data can also be used as an instrument of power.[4] Hostile actors can weaponize information, using antagonistic strategic narratives on social media to undermine public confidence in governments, confuse societal discourses, and exacerbate socio-political divisions.[5]

Since the inception of cyberspace, states have struggled to regulate these novel activities in this domain. Whilst all states agree that international law applies to cyberspace,[6] *how* it applies remains a matter of dispute. Malign actors in cyberspace can (mis)use the legal uncertainty – or grey zone – created by the eclectic interpretation of international law.[7]

This line of reasoning has fuelled the assumption that the next war will be a cyberwar. However, as of 24 February 2022, the 'next war' started with Russia's invasion of Ukraine. This appears to be a predominantly kinetic military war and not a grey zone cyber operation. However, a closer look reveals a multi-layered use of instruments of power, including both

1 Lennart Maschmeyer, 'The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations', *International Security,* Volume 46, Issue 2 (2021): 51–90.

2 Chimene Keitner, 'Foreign Election Interference and International Law', in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Duncan B. Hollis and Jens David Ohlin (Oxford University Press, 2021), 179–95.

3 Kim Zetter, 'Wiper in Ukraine Used Code Repurposed From WhiteBlackCrypt Ransomware', *Zero Day,* January (2022).

4 Miranda Lupion, 'The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News', *Journal of Slavic Military Studies,* Volume 31, Issue 3, (2018): 329–53.

5 Antagonizing narratives exploit vulnerabilities in a society, including latent historical grievances, contentious societal issues, or spontaneous moments of societal uncertainty or tension. See Aiden Hoyle et al., 'Grey Matters: Advancing a Psychological Effects-Based Approach to Countering Malign Information Influence', *New Perspectives,* Volume 29, Issue 2, (2021): 144–64, pp. 146–147; Alexander Lanoszka, 'Russian Hybrid Warfare and Extended Deterrence in Eastern Europe', *International Affairs,* Volume 92, Issue 1, (2016): 175–95, pp. 181–187.

6 Related to international law, regulating state conduct in cyberspace is the core theme of the UN Governmental Group of Experts, the Open-Ended Working Group, but also for the International Group of Expert working on the Tallinn Manual iterations, see e.g. Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017).

7 Michael N. Schmitt, 'Grey Zones in the International Law of Cyberspace', *The Yale Journal of International Law,* Volume 42, Issue 2, (2017): 1–21.

military and informational or cyber means.[8] Moreover, new tropes, techniques and tactics are in evidence in the Russo-Ukraine war, such as the involvement of hackers and ICT firms. Although the evolution of cyberspace activities and the range of actors provide welcome support for Ukraine, they correspondingly pose challenges as these new techniques can expand the grey zone and complicate the coherent application of international law.

This discourse illustrates the main question addressed by this Hybrid CoE Paper: How does the exploitation of new tropes, techniques and tactics in or via cyberspace affect the application of international law to cyber operations within the framework of hybrid warfare? The paper reflects on cyber activities in the context of the Russo-Ukraine war. The second section below provides an overview of cyber activities that could reasonably be expected during the Russo-Ukraine war, but also some new tropes, techniques and tactics. The third section assesses how the new tropes, techniques and tactics affect the legal aspects of hybrid warfare. In the fourth and final part, the impact of exploiting cyberspace will be explored, resulting in consequences that NATO and the EU will have to take into account.

8 The Russian Federation does not use cyber activities but rather information-technology and information-psychological warfare, see Keir Giles, 'Handbook of Russian Information Warfare', *NATO Defence College*, Volume 9, November (2016): 1–90, p. 9.

New tropes, techniques and tactics

After centuries of conventional warfare in which states or state-like actors have waged wars over territory, the emergence of cyberspace as a domain of engagement has raised the expectation of an upcoming cyberwar. Although the Russo-Ukraine war is not that anticipated cyberwar, the involvement of cyber activities – but also measures related to other instruments of power, diplomatic,[9] informational, legal and economic[10] among others – is significant, making it a contemporary hybrid war.

Cyber activities to shape the battlefield

The current Russo-Ukraine war is, on the one hand, a kinetic military operation using battle-proof but outdated material including artillery pieces, command and control systems, and doctrine.[11] On the other hand, despite opinions to the contrary,[12] cyber operations have formed a substantial part of the wider conflict, especially during the prelude to the 2022 war.[13]

Before the invasion on 24 February, cyber activities were undertaken to shape the battlefield and undermine the faith of the Ukrainian population in the government, media and financial institutions.[14] Government websites were defaced or targeted by DDoS attacks.[15] 'WhisperGate' wiper malware was inserted into the ICT infrastructure of emergency response agencies, which could have destroyed files, rendering the systems inoperable.[16] Binary data can be used to degrade or sabotage the virtual dimension of the targeted audiences' critical infrastructure.[17] Apart from digital sabotage or undermining activities affecting the elements of cyberspace itself (hardware and software), activities can also be executed using cyberspace as a vector to impact the cognitive dimension of the targeted audiences. These so-called digital influence operations affecting cognition[18] often make use of framed or manipulated information – words, images,[19] memes and narratives[20] – purporting to bring about a change in

9 'Russian Warning after Irish Diplomats Expelled Speak out against the War', BBC News, 8 April, 2022, https://www.bbc.com/news/articles/c72z8ewl20lo.
10 Michael Race, 'Ukraine War: Russia Threatens to Stop Supplying Gas If Not Paid in Roubles', BBC News, 31 March, 2022, https://www.bbc.com/news/business-60945248.
11 Seth G. Jones, 'Russia's Ill-Fated Invasion of Ukraine', *CSIS Briefs*, 2022; Lawrence Freedman, 'Why War Fails', *Foreign Affairs*, Volume 101, Issue 4, (2022): 10–23.
12 Editorial Board, 'The Ukraine Crisis Should Make Us Rethink What Cyberwarfare Is', *The Washington Post*, 19 March, 2022.
13 Jenna McLaughlin and Tom Burt, 'A Cyberwar Is Already Happening in Ukraine, Microsoft Analysts Say', NPR, 2022.
14 Alden Wahlstrom et al., 'The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine', Mandiant, 2022.
15 Stephanie Pell, 'Contextualizing Last Week's Malicious Cyber Activities Against Ukrainian Government Websites and Systems', Lawfare, 2022.
16 Tom Burt, 'Malware Attacks Targeting Ukraine Government', Microsoft, January (2022).
17 Andy Greenberg, 'Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine', *Wired*, 2022.
18 Christopher Paul and Miriam Matthews, 'The Russian Firehose of Falsehood Propaganda Model: Why It Might Work and Options to Counter It', RAND Corporation, 2016.
19 Bobby Allyn, 'Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn', NPR, 2022.
20 Elias Götz and Jørgen Staun, 'Why Russia Attacked Ukraine: Strategic Culture and Radicalized Narratives', *Contemporary Security Policy*, Volume 43, Issue 3, (2022): 482–97.

attitude. In the prelude to the war, Russia constructed a narrative to 'demilitarize' and 'denazify' Ukraine, appealing to World War II sentiments. Moreover, personal data that had been hacked was leaked into the public domain, and Ukrainians received text messages claiming that ATM services had been disrupted.21 Many of these techniques had been used earlier, in the aftermath of the 2014 annexation of Crimea, but also during the 2016 US presidential election.

New ways of warfare: Hackers, firms, and challenges to virtual sovereignty

Apart from the confluence of cyber and kinetic operations in the Russian use of force, new grassroots *modus operandi* emerged during the war, which challenge our conventional wisdom on activities in cyberspace.[22] While the Russo-Ukraine war is, in essence, and according to international law, an armed conflict between two states, in reality many more actors are involved in a variety of novel activities. **Numerous non-state actors, sympathizers (hacker groups such as Anonymous) and commercial enterprises are taking sides with one of the warring states without necessarily being belligerent entities.** In September, some 35 hacker groups were engaged in cyber activities sympathizing with Ukraine, and 43 in support of Russia.[23] The hacker group 'IT Army' of Ukraine had posted a target list of Russian government email addresses on Twitter, urging hackers to carry out DDoS attacks.[24] Although some of these groups could be affiliated with a state, most of these sympathizers – such as Anonymous affiliates, the Conti group or RedBandit – are private endeavours, and although they side with one of the warring states, their actions are generally not coordinated with those states.

Apart from cyber-sympathizers, another novelty is that commercial ICT firms have entered the virtual battlespace. ICT firms (e.g. Microsoft) in general support and protect the ICT systems of their clients, including the Ukrainian government, and operate discreetly to prevent (or enable recovery from) intrusions. Contrary to previous practices, Microsoft has come forward and made the threats and intrusions public as a form of civic 'naming and shaming'.[25] But they are not alone. After Russia sabotaged the Viasat satellite system,[26] Elon Musk offered his Starlink to avoid further

21 Joseph Marks and Aaron Schaffer, 'The Cyber Fight in Ukraine Is Getting More Serious', *The Washington Post*, 16 February, 2022.

22 Kristen E. Eichensehr, 'Ukraine, Cyberattacks, and the Lessons for International Law', *American Journal of International Law Unbound* 116, (2022): 145–49.

23 The affiliation of 5 groups was unknown. The number and affiliations change over time. Cyberknow, 'Update 20 September 2022 Russia-Ukraine War – Cyber Group Tracker', https://twitter.com/hashtag/cybertracker?src=hashtag_click.

24 Brett Callow, Twitter post, '"The IT Army"' Announced by Minister for Digital Transformation of Ukraine Mykhaylo Fedorov Has Released Its Target List', 26 February, 2022.

25 Digital Security Unit, 'Special Report : Ukraine – An Overview of Russia's Cyberattack Activity in Ukraine', Microsoft, 2022; Martha Finnemore and Duncan B. Hollis, 'Beyond Naming and Shaming: Accusations and International Law in Cybersecurity', *European Journal of International Law,* Volume 31, Issue 3, (2020): 969–1003.

26 Council of the EU, 'Russian Cyber Operations against Ukraine: Declaration by the High Representative on Behalf of the European Union', Press Release (2022), https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

internet outages, responding to a Twitter message by the Ukrainian Minister of Digital Transformation, Mykhailo Fedorov.[27] The communication infrastructure was not completely disrupted by Russia, not least since their own military depended on it.[28] Furthermore, cyber-related interest groups and civilian initiatives including Mandiant or Bellingcat have taken a more forward-leaning posture, siding against Russia.

Finally, Russia is not only trying to seize Ukrainian territory in a physical manner, but also challenging the virtual sovereignty of the occupied Eastern provinces in Ukraine.[29] By changing the country code from .ua to .ru, the internet traffic will follow different routes and gateway protocols and thus fall under Russian digital control and possibly jurisdiction.[30]

A follow-on effect is that intelligence services,[31] traditionally operating covertly, are sharing intelligence on the situation in Ukraine on Twitter. These insights will not only serve the Ukrainian forces and deter Russian actors, they will also shape the perceptions of NATO and EU populations and will inform commercial and civilian actors virtually or physically engaged in the Ukrainian battlespace.

In sum, from the Russian perspective, cyber operations in the Russo-Ukraine war were used to shape the 'battlefield'. After a predominantly kinetic phase of the war in the days after 24 February, cyber operations coalesced with traditional military warfare as of mid-March.[32] Cyber activities of both warring states followed the course of the war, supporting or enhancing the kinetic military operations in a more or less coordinated manner.[33] The Russo-Ukraine war also demonstrated new ways of exerting power. The proactive involvement of non-state hackers, and the participation of ICT businesses siding with one of the belligerent parties were not foreseen.

27 Elon Musk, Twitter post, 'Starlink Service Is Now Active in Ukraine', 27 February 2022, https://twitter.com/elonmusk/status/1497701484003213317?s=11.

28 Von Jakob Lindern, '"Die Russischen Soldaten Brauchen Selbst Strom" (Interview Mit Matthias Schulze)', *Zeit On Line*, 2022.

29 Herbert S. Lin, 'The Emergence of Physically Mediated Cyberattacks?', Lawfare, 2022.

30 Adam Satariano and Scott Reinhard, 'How Russia Took Over Ukraine's Internet in Occupied Territories', *The New York Times*, 9 August, 2022, https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html.

31 United Kingdom Ministry of Defence, Twitter post, 'Latest Defence Intelligence Update on the Situation in Ukraine – 8 April 2022', 8 April 2022, https://twitter.com/DefenceHQ/status/1512284278813597702.

32 David Cattler and Daniel Black, 'The Myth of the Missing Cyberwar', *Foreign Affairs*, 2022.

33 The lack of coordination was possibly due to the fact that after 24 February 2022, the RF had planned to execute a 3-day military campaign to capture Kiev. In that period, no specific cyber activities were required. Cyber actions were revigorated after the 3-day objective failed. See also Robert Johnson, 'The First Phase of the Russian Invasion of Ukraine 2022', Oxford Changing Character of War Centre, 2022.

Scope and effect of cyber operations

One of the aspects of the contemporary hybrid conflict is the use of the legal instrument of power,[34] especially if international law can be interpreted to serve one's purposes. Diverging interpretations and the subsequent ambiguity are nothing new and are certainly not instigated by cyberspace.[35] Even in the current war, the legal instrument has been used by Russia invoking the right of (collective) self-defence by the 'independent' People's Republics of Luhansk and Donetsk to justify invading Ukraine,[36] but also announcing a referendum in the Donbas region appealing to the generally accepted principle of the self-determination of peoples.[37] However, **the emergence of cyberspace has increased legal uncertainty. States are struggling with *how* to regulate activities in cyberspace.**

Increased legal uncertainty in cyberspace

There a several legal stumbling blocks in the application of international law to cyberspace, one of which relates to sovereignty in cyberspace. While most states argue that sovereignty is a principle *and* a legally binding rule in cyberspace as it is in other domains, the United Kingdom (UK) is not convinced that sovereignty is more than a principle in cyberspace.[38] Another stumbling block is due diligence; in recent UN talks,[39] this acknowledged rule of customary international law has been 'downgraded' to a voluntary norm for activities in cyberspace. The challenge of applying international law to cyberspace also provided the impetus for a group of academics to share their interpretations in the so-called *Tallinn Manual*, encouraging states to forward their legal opinions.[40] Agnostic as to which discourse reflects the correct interpretation of international law with regard to cyberspace, the diverging legal opinions in themselves create uncertainty.[41]

The expectation was that over the course of time, acts of state behaviour and expressions of legal opinion would crystallize *how* to apply

34 Charles J. Dunlap, 'Lawfare 101', *Military Review*, May-June, (2017): 8–9.

35 An earlier example relates to the legal difference between the use of force and an armed attack. After the 1986 *Nicaragua Case, the United States has aligned the two notions, while for most (European) states they differ in scale and effect,* subsequently implying different responses. See 'Case Concerning Military and Paramilitary Activities in and against Nicaragua', ICJ Reports (1986).

36 James A. Green, Christian Henderson, and Tom Ruys, 'Russia's Attack on Ukraine and the Jus Ad Bellum', *Journal on the Use of Force and International Law*, 2022; Michael N. Schmitt, 'Russia's 'Special Military Operation' and the (Claimed) Right of Self-Defense', *Articles of War*, Issue 1.

37 Pavel Polityuk, Humeyra Pamuk, and Caleb Davis, 'Putin Orders Mobilisation for Ukraine War in What West Calls Desperate Act', Reuters, 21 September, 2022, https://www.reuters.com/world/europe/ukraine-marches-farther-into-liberated-lands-separatist-calls-urgent-referendum-2022–09–19/.

38 Jeremy Wright, 'Cyber and International Law in the 21st Century', 2018; Suella Braverman, 'International Law in Future Frontiers', Chatham House, 2022.

39 See para 13 c of the United Nations GGE 2021 Report, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – A 76/135', (May 2021): 10.

40 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.*

41 See also Schmitt, 'Grey Zones in the International Law of Cyberspace', 4–7.

international law to cyberspace.[42] But paradoxically enough, **while the number of legal opinions has increased,[43] so have the divergences in interpretation, generating more and not less ambiguity.** Aside from the UK position on sovereignty, those states that affirm that sovereignty is a binding legal rule also differ in the breadth of application of the rule. While France and Switzerland regard any incursion into ICT infrastructure as a breach of sovereignty,[44] Canada, the Netherlands and Germany argue that negligible effects below a certain threshold will not per se constitute such a violation.[45]

The result of this increased uncertainty is that states that fall victim to a cyberattack query what the proper and lawful response to these attacks – which often remain below the threshold of the threat or use of force – should be.[46] Related to sovereignty or due diligence, if one state understands sovereignty as a binding legal rule in cyberspace, it can respond once the rule is breached. Invoking the right to respond to an internationally wrongful act demands that – apart from the quandary of attributing the breach to a state – the attack needs to violate a binding legal rule.[47] However, **if there is doubt over whether the violation concerns a binding legal rule, principle or voluntary norm, responding to the attack could itself be a violation of international law.**

From legal uncertainty to legal asymmetry

War and conflict have accelerated innovation but, similarly, new inventions have changed the character of warfare,[48] and the manner in which we fight and might be required to brush up on international law.[49] In the Russo-Ukraine war, non-state actors make use of the virtual dimension to engage in an armed conflict targeting critical infrastructure or saturating audiences with biased narratives and manipulatively framed messages.[50] Microsoft attributes cyberattacks to state but also non-state actors. Most non-state actors do not engage in

42 See e.g. Harriet Moynihan, 'The Application of International Law to State Cyberattacks – Sovereignty and Non-Intervention', 2019, p. 58. Recommendations to governments; Duncan B. Hollis and Jan Neutze, 'Defending Democracies via Cybernorms', in *Defending Democracies: Combating Foreign Election Interference in a Digital Age*, ed. Duncan B. Hollis and Jens D. Ohlin (Oxford University Press, 2021), 318; Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice', *The American Society of International Law*, Volume 112, Issue 4 (2018): 583–657, pp. 584–585.

43 Michael N. Schmitt, 'Taming the Lawless Void: Tracking the Evolution of International Law', *Texas National Security Review,* Volume 3, Issue 3 (2020): 34.

44 Swiss Ministry of Foreign Affairs, 'Position Paper on Switzerland's Participation in the UN OEWG and UNGGE', (2020); Ministère des Armées, 'Droit International Appliqué Aux Opérations Dans Le Cyberespace', 2019.

45 See e.g. German Ministry of Foreign Affairs, 'On the Applicability of International Law in Cyberspace', 2021, p. 4.

46 As recognized in Article 2(4) of the United Nations, 'Charter of the United Nations' (1945).

47 Article 2 of the Responsibility of States for Internationally Wrongful Acts. See James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*, ed. James Crawford (Cambridge: Cambridge University Press, 2002).

48 MacMillan, *War: How Conflict Shaped Us*, 62–64.

49 Legality of the Threat or Use of Nuclear Weapons – Advisory Opinion of 8 July 1996, ICJ Reports (1996).

50 Wahlstrom et al., 'The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine'.

violent attacks,[51] operate from outside Russia or Ukraine, and can seldom be connected to any specific territory or location – hacker groups are often collections of individuals using cloud-based techniques. **The non-state actors cannot be attributed to a state, and do not directly participate in the hostilities, at least not physically; hence their status in international law is difficult to determine.**

The tropes, techniques and tactics used in the Russo-Ukraine war have also provided new dynamics in the interplay between cyber operations and international law. The exploitation of cyberspace even appears to be at odds with the characteristics of traditional state behaviour in the international context and thus with (customary) international law, which guides the coexistence and cooperation between states. **International law is based on the state, a territory, and the distinction between war and peace, while cyberspace is not.** In the past, efforts have been made to connect 'an actor' to 'a state' in order to make international law applicable to the situation at hand. **The Russo-Ukraine war has made it clear that as this connection to a state actor oftentimes does not exist, standards of international law such as sovereignty and non-intervention are difficult to apply in cyberspace.[52]** International law, especially the notion of territorial integrity as a part of the rule of respect for sovereignty in international affairs, has a strong territorial connection, in contrast to many virtual activities in cyberspace.[53] Remotely executed cyber operations often pursue goals other than causing physical damage or impairment.[54]

Finally, the attributes of cyberspace have also transformed the dichotomy between war and peace into a sliding scale of grey shades;[55] differences between kinetic and non-kinetic acts and effects, but also between domestic and international behaviour, are ever more difficult to discern.

The new tropes, techniques and tactics as materialized in the Russo-Ukraine war have only added to the complexity of how to apply international law to cyberspace. **The differences in interpretations may provide 'opportunities' to use the law as an instrument of state power.** Uncertainties can be exploited, creating legal asymmetry, hence the ability to interpret the international legal framework in such a manner that it provides leverage for the aggressor while simultaneously limiting (often self-imposed) the opposing actor. While Russia violated US sovereignty and possibly the prohibition of non-intervention during the 2016 presidential election, the US was restrained when it came to responding, not least out of fear of escalation.[56] Reticence towards Russian cyber activities

51 Article 49 of the Additional Protocol (AP I) to the Geneva Conventions, relating to the Protection of Victims of International Armed Conflicts.

52 Except for International Humanitarian Law or International Human Rights Law, which can also apply to non-state actors. Beyond international law, national law regimes can be applied in e.g. criminal offences.

53 Peter B.M.J. Pijpers and Bart G.L.C. Van Den Bosch, 'The 'Virtual Eichmann': On Sovereignty in Cyberspace', ACIL Research Paper 2020–65, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3746843.

54 Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Rule 4, 17–27.

55 Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017).

56 William Banks, 'State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0', *Texas Law Review,* Volume 95, Issue 7, (2017): 1487–1513, p. 1498; Barrie Sander, 'Democracy under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', *Chinese Journal of International Law,* Volume 18, Issue 1, (2019): 1–56, p. 53.

was already observed during the 2015 Ukrainian power grid outage caused by BlackEnergy malware,[57] or the interference during the 2017 French presidential election and the 2018 Italian election.[58]

57 Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *Wired*, 2016.
58 Lauren Speranza, '#ElectionWatch: How Russia-Italy Relations Are Impacting the Italian Elections', Atlantic Council, 2018.

Exploiting cyberspace: The asymmetric nature of future conflicts?

The developments described above will not stop in the near future. Technological developments (AI or quantum computing) will outpace our intellectual elasticity to absorb these developments.[59] Or, as Lin stated, '(a)lthough the volume and velocity of information has increased by orders of magnitude in the past few decades, the architecture of the human mind has not changed appreciably in the last few thousand years, and human beings have the same cognitive and perceptual limitations that they have always had'.[60]

The new tropes, techniques and tactics have an impact on the ability to use and exploit cyberspace. This has consequences for NATO and the EU, and there are elements that need to be taken into account for future conflicts.

1. **There is an increasing amalgamation of the instruments of power during competition and conflict.** Kinetic and cyber activities go hand in hand during conflicts, while most Western states still perceive, assess and train the application of diplomatic, economic, informational or military measures in stovepipes, sometimes induced by the democratic separation of powers. Although NATO and the EU (member states) should not follow autocratic examples, they should share information and intelligence between state agencies and should also consider **sharing data with private actors**, not least since private actors sometimes have embedded situational awareness and a better access position than state agencies. The Russo-Ukraine war has made it clear that **faster and more transparent sharing of information is vital for success**.
2. **International law is applicable to cyberspace, but it appears that cyberspace is not compatible with international law.** When related to conflict and competition, there is a growing parallax between the foundations of international law and the attributes of cyberspace. While international law is built on the notions of the state, territory, and the division between war and peace, the Russo-Ukraine war made it clear that **cyberspace is increasingly blurring the lines between state and non-state actors, the virtual and physical world, and thrives in the grey zone between war and peace.** NATO and the EU should not cope with these threats separately. Instead of competing over notions like a European Army, NATO and the EU should complement each other, based on their founding principles and inherent (military, diplomatic and economic respectively) strengths.
3. **Diverging interpretations on how to apply international law to cyberspace create legal ambiguity and uncertainty.** This means that the latitude or leverage that states have to defend their vital interests differs based on – often stringent and sometimes self-inflicted – national interpretations of international law. Intentionally exploiting these variances will create legal asymmetry, and hence an instrument of power for a state. Therefore, following the Scandinavian example, NATO

59 In 2018 the UK Attorney General stated that: 'One of the biggest challenges for international law is ensuring it keeps pace as the world changes.' Wright, 'Cyber and International Law in the 21st Century'.

60 Herbert S. Lin, 'Developing Responses to Cyber-Enabled Information Warfare and Influence Operations', Lawfare, 2018.

and the EU could align their legal interpretations of international law applicable to cyberspace. NATO and the EU can take common positions on parts of international law during international state-level legal conferences, and follow a spill-over approach from there, reaching agreement on other parts of regimes of international law. If not, by providing diverging interpretations of the law, NATO and EU member states may in fact craft the perfect weapon for malicious actors to exploit cyberspace.

Author

Peter B.M.J. Pijpers, PhD is an Associate Professor of Cyber Operations at the Netherlands Defence Academy and a researcher at the Amsterdam Centre of International Law (ACIL), University of Amsterdam. Corresponding address: b.m.j.pijpers@uva.nl.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats