The Ukraine Crisis as a Test for Proposed Cyber Norms

by
Henry Rõigas

Chapter 15 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

In Chapter 15, NATO CCD COE researcher Henry Rõigas discusses the impact of known cyber attacks in Ukraine on proposed political cyber 'norms', the rules of state behaviour in international relations. On the positive side, the absence of attacks against critical infrastructure could be a boon to future international security and stability, especially if it is a result of intentional restraint on the part of Moscow and Kyiv. This case challenges the prevailing perception that a loose normative framework currently allows states to employ cyber attacks as a tool for coercion. On the negative side, the examples of computer network operations we have seen appear to violate the information security norms promoted by Russia and the Shanghai Cooperation Organisation (SCO), as they seem to constitute a war on information itself, that is a dedicated effort to alter public opinion through deceptive propaganda.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

The Ukraine Crisis as a Test for Proposed Cyber Norms

Henry Rõigas
NATO CCD COE

1 Introduction

In international forums, governments, academia, and the private sector have strenuously argued that states must agree on existing or develop a set of international norms for conflict in cyberspace. Our current environment is characterised by a steep rise in the development of offensive cyber tools and tactics – as well as a general disagreement on when and where it is appropriate to use them. The overall result is a popular perception of a weakened international security environment that threatens to devolve into an anarchic Hobbesian world of 'all against all'. Against this backdrop, there have been urgent calls for greater investment in cyber diplomacy.[1]

The term 'norm' has become somewhat of a buzzword in these discussions used to argue that states should adhere to certain rules of behaviour with regard to conducting cyber operations. This chapter will thus first describe the nature of 'cyber norms' and then discuss the primary developments in the global arena. The author's focus will be on the *proposed* cyber norms of behaviour that would have a politically binding character, and will avoid discussing *existing* international law

The term 'norm' has become somewhat of a buzzword.

1 See, for example, developments in the United Nations: http://www.un.org/disarmament/topics/informationsecurity/, and The Council of the European Union's conclusions on cyber diplomacy: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

(legal norms)[2] as well as the challenges of practical implementation of the these norms.

Finally, this chapter will analyse the Ukraine crisis in light of these proposals, and attempt to assess their rationality and applicability. The Russo-Ukrainian conflict, in theory, offers a suitable case study in that there has been ample room for malicious state-sponsored cyber activities: first, nation-states perceived as having considerable cyber capabilities – not only Russia and Ukraine, but also surrounding nations and the member states of NATO – are involved, at least indirectly; and second, the crisis has both endured and evolved from the Euromaidan street protests to the Russian annexation of Crimea to open, armed conflict in eastern Ukraine.

2 Proposed 'Political' Cyber Norms

In international relations, norms are often defined as 'collective expectations of proper behaviour for an actor with a given identity',[3] which is broad enough that states (and other stakeholders) use the term to put forward a wide range of proposals in diplomatic forums. This chapter takes a simplified approach, limiting its scope to (1) legal and (2) political norms: the 'proper behaviour' of states is comprehensively regulated by international law (i.e. *legal* norms such as treaties, international customs, and general principles of international law)[4] and through cyber diplomacy in the form of *political* or non-legally binding agreements. The United Nations Group of Governmental Experts (UN GGE) has explained the nature of these politically binding instruments by stating that 'norms reflect the international community's expectations, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States'. The problem, of course, is that breaches of such political norms only give rise to political, non-legal consequences.[5]

> *Norms reflect the international community's expectations, set standards for responsible State behaviour.*

There has been some agreement between nation states on setting international 'cyber norms'. In 2013, the UN published an accord, written by a GGE including representatives from the US, UK, China, and Russia, expressing consensus on the

2 For a discussion on the role of legal cyber norms, see Michael N. Schmitt and Liis Vihul. 'The Nature of International Law Cyber Norms,' *Tallinn Papers*, no. 6 (2014), https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf.

3 See Martha Finnemore and Kathryn Sikkink. 'International Norm Dynamics and Political Change,' *International Organization* 52, no. 4 (October 1, 1998): 887–917.

4 See sources of international law listed in the Statute of the International Court of Justice (ICJ), Article 38.

5 Some have also used the terms 'hard' and 'soft' law in this context, see Dinah Shelton. 'Normative Hierarchy in International Law', *The American Journal of International Law* 100, no. 2 (April 1, 2006): 291–323. For a concept listing policy responses to cyber incidents, see Tobias Feakin. 'Developing a Proportionate Response to a Cyber Incident' *Council on Foreign Relations*, August 2015, http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber-incident/p36927.

basic notion that existing international law applies to cyberspace.[6] In 2015, the same forum published another report[7] which delved into greater detail, but the GGE has previously not elaborated on precisely how to apply existing laws (legal norms) to the nuanced field of cyber security. The reports did state, however, that the unique attributes of information and communications technology (ICTs) could demand the creation of altogether new norms.

The fairly general agreement expressed in the reports can be viewed both as the lowest common denominator between the world's key cyber powers and as a manifestation of a general lack of clarity in this new geopolitical arena. Meanwhile academia has to some degree filled the void, actively addressing the applicability of existing international law,[8] although work in the area of state practice and interpretation has been relatively limited. In the context of norms restraining state behaviour, existing international law such as the prohibition on the use of force and the law of armed conflict (LOAC) are highly relevant and indispensable, but it is likely that additional norms – political rather than legal – will be developed by the international community over time. Two somewhat opposing approaches to these new political norms will be addressed below.

One group of nations acting as 'norm entrepreneurs'[9] seems to aim for a treaty-level agreement to govern state activities in cyberspace. Member nations of the Shanghai Cooperation Organisation (SCO)[10] have proposed a Code of Conduct for International Information Security[11] to the UN. In parallel, Russia has developed (in 2011) a separate concept for a Convention on International Information Security[12] which covers, to a large extent, the same territory.

These proposed instruments do not apply the prefix 'cyber' when addressing ICT-related issues; instead, the focus is on preserving 'information security' which represents a broad conceptualisation of the threat environment and the scope of limited state activities.[13] According to SCO's own agreement on information security (the Yekaterinburg Agreement of 2009)[14] and the aforementioned Convention proposal by Russia (2011), 'information war' entails, in addition to damaging information systems and critical infrastructures (which is often the 'Western' scope of

6 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/69/723, 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

7 United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 2015, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement.

8 See the Tallinn Manual process: https://ccdcoe.org/research.html.

9 See Finnemore and Sikkink. "International Norm Dynamics and Political Change," October 1, 1998.

10 Member States of the SCO are China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan.

11 United Nations, General Assembly, *Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary-General*, *A/69/723*, 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

12 The Ministry of Foreign Affairs of the Russian Federation. *Convention on International Information Security (Concept)*, 2011, http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument.

13 See, for example, James A. Lewis. 'Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms,' Strategic Technologies Program (Center For Strategic and International Studies, 2014), 6.

14 Annex 1of SCO, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*.

actions when the term 'cyber security' is used), also 'psychologic brainwashing to destabilise society and state', signalling that for them the threat also stems from content and information itself.[15]

The Code of Conduct puts a strong emphasis on the principle of *information sovereignty*,[16] arguing that states should not use 'ICTs and information and communication networks to interfere in the internal affairs of other states or with the aim of undermining their political, economic and social stability'. It asks states to refrain from 'activities which run counter to the task of maintaining international peace and security' and highlights a state's responsibility to protect 'information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage'. Further, it includes a section that prohibits states from using 'dominant position in ICTs' to engage in the aforementioned activities. In terms of international cooperation, the Code seeks to curb 'the dissemination of information that incites terrorism, separatism or extremism'.

Documents demonstrate the ambition of SCO members to see a treaty-level agreement.

These documents demonstrate the ambition of the SCO members to see an eventual treaty-level agreement. However, if the Code of Conduct would actually be adopted in the current form, it could not be considered as a source of international law (a legal instrument) since the norms are of a politically binding character due their 'aspirational' and non-compulsory nature.[17]

The Code of Conduct has not been put to a vote as adoption at the UN is highly unlikely due to opposition from many liberal democracies. An alternative strategy, promoted initially by the US, is to strengthen international cyber security through voluntary norms of behaviour that pertain during peacetime.[18] According to this logic, most cyber operations fall below the 'use of force' threshold, which means that most of the existing legal norms regulating interstate cyber operations are not sufficient.[19] During the height of the cyber incidents in Ukraine, the US promoted the fol-

An alternative strategy is to strengthen international cyber security through voluntary norms.

15 See, for example, Keir Giles. 'Russia's Public Stance on Cyberspace Issues,' in *2012 4th International Conference on Cyber Conflict*, ed. Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (NATO CCD COE Publication, 2012), http://www.ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

16 See the Chinese viewpoint in Lu Wei. 'Cyber Sovereignty Must Rule Global Internet,' *The Huffington Post*, December 15, 2014, http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html.

17 Schmitt and Vihul. 'The Nature of International Law Cyber Norms,' 4.

18 States supporting this view strongly emphasise the applicability of existing international law and see that these norms should be 'voluntary measures of self-restraint' during peacetime, see Christopher M. E. Painter. *Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues, U.S. Department of State Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy Hearing Titled: 'Cybersecurity: Setting the Rules for Responsible Global Behaviour,'* 2015, http://www.foreign.senate.gov/imo/media/doc/051415_Painter_Testimony.pdf.

19 *Ibid*., 8–9. Also, see Tallinn Manual 2.0 process focusing on international law applicable to cyber operations that do not mount to an 'use of force' or do not take place during armed conflict, https://ccdcoe.org/research.html .

lowing four norms of which the first three were included in the recent UN GGE report:[20]

(1) states should not conduct or knowingly support online activity that damages or impairs critical infrastructure (norm 1);
(2) states should not conduct or knowingly support activity intended to prevent the national Computer Security Incidents Response Teams (CSIRTs or CERTs) from responding to cyber incidents, nor use CSIRTs to do harm (norm 2);
(3) states should cooperate with other states in investigating cybercrime by collecting electronic evidence and mitigating cyber activity emanating from its territory (norm 3); and
(4) states should not conduct or knowingly support cyber-enabled theft of commercially valuable intellectual property (norm 4).

Before we move on, it is important to note that these and other cyber norms have been analysed in academic circles[21] as well as in the private sector. For example, Microsoft has recommended six cybersecurity norms designed to limit the proliferation of cyber weapons and offensive operations in cyberspace.[22]

3 Observations from Ukraine: Hints of State-sponsored Operations

The attribution of cyber attacks is notoriously difficult. In order to discover state-sponsored operations, one can only speculate based upon inconclusive indicators such as target, malware, motive, and complexity.

In Ukraine, some advanced cyber espionage tools such as Turla/Snake/Ourobours and Sandworm have not only been linked to the conflict, but also associated with an 'Advanced Persistent Threat' (APT) actor (i.e. nation-state), likely Russia.[23] At the same time, analysts have argued that *most* of the cyber attack methods in Ukraine such as DDoS attacks and defacements have been technically unsophisticated. Thus, on balance, the 'complexity criterion' appears unmet.

20 Painter. *Testimony of Christopher M. E. Painter, Coordinator for Cyber Issues, U.S. Department of State Before the Senate Foreign Relations Committee Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy Hearing Titled: 'Cybersecurity: Setting the Rules for Responsible Global Behaviour.'*

21 For example, drawing parallels with state obligations during crises on the sea, a duty to assist victims of severe cyberattacks (an e-SOS) has been proposed by Duncan B. Hollis in 'An E-SOS for Cyberspace,' *Harvard International Law Journal* 52, no. 2 (2011), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1670330.

22 Angela McKay *et al.*, 'International Cybersecurity Norms. Reducing Conflict in an Internet-Dependent World' (Microsoft, 2015), http://download.microsoft.com/download/7/6/0/7605D861-C57A-4E23-B823-568CFC36FD44/International_Cybersecurity_%20Norms.pdf.

23 See, for example, 'Suspected Russian Spyware Turla Targets Europe, United States,' *Reuters*, March 7, 2014, http://www.reuters.com/article/2014/03/07/us-russia-cyberespionage-insight-idUSBREA260YI20140307; 'Zero Day Vulnerability CVE-2014-4114 Used in Cyber-Espionage,' *iSIGHT Partners*, October 21, 2014, http://www.isightpartners.com/2014/10/cve-2014-4114/.

Actions attributed to hacktivist groups raise questions regarding possible coordination with state entities.

Actions attributed to hacktivist groups also raise questions regarding possible coordination with state entities. For example, Ukrainian officials reported that, even when the hacktivist group CyberBerkut failed to compromise Ukraine's online election system and only managed to present fake election results on the election's website for a very brief period, a Russian state-owned TV channel still displayed these results immediately.[24] In another incident, CyberBerkut allegedly leaked the recording of a phone call between Estonian Minster of Foreign Affairs Urmas Paet and European Union (EU) High Representative for Foreign Affairs and Security Policy Catherine Ashton, suggesting that Cyber Berkut either possesses sophisticated cyber capabilities or has links to Russian intelligence services.[25]

Here, we must remember SCO's focus on 'information security', as opposed to 'cyber security', and in fact many analysts believe that both Russia[26] and Ukraine[27] are conducting information operations within the context of the ongoing conflict in eastern Ukraine. The internet is a natural terrain for these operations;[28] the reported 'troll factories' in St. Petersburg creating pro-Russian comments for online new media serve as prominent examples.[29]

4 Which Norms of Behaviour Were Followed?

Thus, there are two dominant ongoing conversations relative to the creation of political cyber norms: (1) the information security norms proposed by the SCO, and (2) the voluntary norms of behaviour in peacetime (initially promoted by the US). This section will analyse the known cyber incidents in Ukraine in the context of these two normative frameworks.

24 Mark Clayton. 'Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers,' *Christian Science Monitor*, June 17, 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

25 Ewen MacAskill. 'Ukraine Crisis: Bugged Call Reveals Conspiracy Theory about Kiev Snipers,' *The Guardian*, March 5, 2014, http://www.theguardian.com/world/2014/mar/05/ukraine-bugged-call-catherine-ashton-urmas-paet; Trend Micro, 'Hacktivist Group CyberBerkut Behind Attacks on German Official Websites,' *Security Intelligence Blog*, http://blog.trendmicro.com/trendlabs-security-intelligence/hacktivist-group-cyberberkut-behind-attacks-on-german-official-websites/.

26 NATO StratCom Centre of Excellence, *Analysis of Russia's Information Campaign Against Ukraine*, October 15, 2014, http://www.stratcomcoe.org/download/file/fid/1910.

27 Maksim Vikhrov. 'Ukraine Forms 'Ministry of Truth' to Regulate the Media,' *The Guardian*, December 19, 2014, http://www.theguardian.com/world/2014/dec/19/-sp-ukraine-new-ministry-truth-undermines-battle-for-democracy.

28 Maeve Shearlaw. 'From Britain to Beijing: How Governments Manipulate the Internet,' *The Guardian*, April 2, 2015, http://www.theguardian.com/world/2015/apr/02/russia-troll-factory-kremlin-cyber-army-comparisons.

29 Dmitry Volchek and Daisy Sindelar. 'One Professional Russian Troll Tells All,' *RadioFreeEurope/RadioLiberty*, March 25, 2015, sec. Russia, http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html; Shearlaw. 'From Britain to Beijing.'

4.1 The Information Security Norms Proposed by the SCO

In general, the state-sponsored conventional military operations in Ukraine are not in accordance with international norms;[30] therefore, it should come as no surprise that the reported cyber incidents also appear unorthodox. However, one important question, given that Russia is directly involved in the Ukraine conflict, is how these cyber incidents fit into the Code of Conduct framework whose primary focus is information sovereignty. In that regard, alleged Russian cyber operations would appear inconsistent with the norms it has hitherto proposed or supported. In fact, most of the cyber incidents reported by both sides in the conflict seem to fall into the category of information operations, which could be interpreted as violating another state's information sovereignty. In the words of the Code of Conduct, ICTs were likely used in an effort to interfere 'in the internal affairs of other States […] with the aim of undermining their political, economic and social stability'.

Alleged Russian cyber operations appear inconsistent with the norms it has hitherto proposed.

Since the norms supported by SCO and Russia focus on 'information' rather than strictly 'cyber' security, one can see that the non-cyber information operations via other media such as TV are also inconsistent with the stated principle of information sovereignty. The Code of Conduct also prohibits the abuse of a 'dominant position' in cyberspace; in this regard too, Russia may have violated its own principles by abusing its control over Russian-owned social media networks such as *Vkontakte* and *Odnoklassniki* which are also popular among Ukrainian users.[31]

Analysing the application of the SCO-proposed information security norms reveals an inherent weakness: quantifying the influence of highly subjective information content or identifying a breach of 'information sovereignty' is problematic, if not impossible.

4.2 The Voluntary Norms of Behaviour in Peacetime

The voluntary, politically binding norms advocated by the US (and partly recommended by the UN GGE) are intended to apply in peacetime. Nonetheless – and however one classifies the Ukraine conflict from a legal perspective[32] – we can still speculate relative to their application during a time of conflict.

In Ukraine, the most important observation so far is that no destructive cyber attacks on critical infrastructure (CI) have been reported by either side. To some degree, this offers hope that the norm of limiting cyber attacks against CI could

30 See collection of legal arguments related to the use of force in the Ukraine conflict, 'Debate Map: Ukraine Use of Force,' accessed August 17, 2015, http://opil.ouplaw.com/page/ukraine-use-of-force-debate-map.

31 Margarita Jaitner and Peter A. Mattsson. 'Russian Information Warfare of 2014,' in *2015 7th International Conference on Cyber Conflict*, ed. Markus Maybaum, Anna-Maria Osula, and Lauri Lindström (NATO CCD COE Publication, 2015), 39–52; 'Vkontakte Founder Flees Russia, Claims Persecution,' *The Moscow Times*, April 22, 2014, http://www.themoscowtimes.com/news/article/vkontakte-founder-flees-russia-claims-persecution/498715.html.

32 See Chapter 14 by Jan Stinissen.

This offers hope that the norm of limiting cyber attacks against CI could evolve into a standard of behaviour.

evolve into a standard of behaviour.[33] A possible exception is the alleged sabotage of the Ukrainian election system, but even here, one might disagree over whether this was a simple information operation or a serious attack against CI.[34] The pertinent question here may relate to the proper definition of CI.

Historically, there have been some significant network intrusions,[35] but relatively few examples of effective cyber attacks against CI.[36] The few cases that are presented as destructive state-sponsored attacks – Stuxnet being the best-documented example[37] – can still be seen as outliers. With that in mind, even well-established norms are mere 'collective expectations of proper behaviour'[38], and it is unrealistic to assume that every actor (especially a nation at war) would always abide by them.

Assuming there have been no attacks against CI in Ukraine, can we say that this is another example of cyber powers restraining themselves?[39] First, this restraint may be strongly influenced by case-specific factors, as explained by Martin Libicki in Chapter 12. Second, one can identify more universal reasons stemming from classical realpolitik calculus of state actors. Is it possible that cyber does not give nation-states a revolutionary way to damage CI (or otherwise harm the citizens of an adversary state) for strategic gain?[40] Or does the case of Ukraine show that cyber operations are now universally employed, but less effective than feared?[41] In other words, the tactical opportunities that cyber is often seen as providing – the infinite reach, low cost of entry, and plausible deniability – may not easily translate to the strategic level.[42] This is also apparent as there

Is it possible that cyber does not give nation-states a revolutionary way to damage CI for strategic gain?

33 Limiting attacks against CI was also covered in the aforementioned SCO's Code of Conduct.

34 Clayton. 'Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers (+video).'

35 See, for example, Trend Micro and Organization of American States. 'Report on Cybersecurity and Critical Infrastructure in the Americas,' 2015, http://www.trendmicro.com/us/security-intelligence/research-and-analysis/critical-infrastructures-security/index.html?cm_mmc=VURL:www.trendmicro.com-_-VURL-_-/oas/index.html-_-vanity; Jack Cloherty et al., "'Trojan Horse' Bug Lurking in Vital US Computers,' *ABC News*, November 7, 2014, http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476; 'Havex Malware Strikes Industrial Sector via Watering Hole Attacks,' *SC Magazine*, June 25, 2014, http://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/357875/.

36 Thomas Rid. *Cyber War Will Not Take Place* (Oxford ; New York: Oxford University Press, 2013); Brandon Valeriano and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford ; New York: Oxford University Press, 2015).

37 David E. Sanger. 'Obama Ordered Wave of Cyberattacks Against Iran,' *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

38 Finnemore and Sikkink. "International Norm Dynamics and Political Change," October 1, 1998.

39 Valeriano and Maness. *Cyber War versus Cyber Realities*; Rid, *Cyber War Will Not Take Place*.

40 For a collection of authors challenging the cyber threat perception, see 'The Cyberskeptics,' *Cato Institute*, http://www.cato.org/research/cyberskeptics.

41 Rid. *Cyber War Will Not Take Place*; Valeriano and Maness. *Cyber War versus Cyber Realities*.

42 See similar remarks made by Jason Healey at Atlantic Council's panel on 'Waging Cyber Conflict', https://www.youtube.com/watch?v=aTKk4CSC9EM.

is still no shortage of 'cyber sceptics',[43] even if the vexing attribution problem were hypothetically to go away.[44]

The Ukraine case study, at least, suggests that cyber has not yet 'changed the game' in terms of state vs. state cyber attacks that destroy physical infrastructure. More likely, it can be understood as one additional weapon in a state's arsenal, and that existing norms – both legal and political – governing traditional state-to-state actions are still followed as if they were applying to other, more conventional attack methods.

As of October 2015, the examples of cyber incidents in the Ukraine crisis allow us to make tentative observations about the other proposed norms of behaviours (2, 3, and 4). In respect of norm number 2, there have been no reported allegations of interference with the work of the national CERTs. However, although some personal communications may have continued, there have been few official CERT to CERT discussions since the conflict began.[45] Against number 3, there have been no published reports of recent Russo-Ukrainian cybercrime investigations,[46] but that may be too much to hope for given that the two countries are currently in open conflict. However, the fact that Russia is unwilling to accede to the Budapest Convention on Cybercrime does not stand in its favour.

The final norm, number 4, which asks states not to steal intellectual property via cyber means, is also likely not followed, given the two countries' current state of hostilities and numerous reports of ongoing cyber espionage. Adopting the norm concerning cyber espionage is in any case fraught with challenges, as its primary norm entrepreneur, the US, has been heavily criticised by both allies and adversaries in the wake of the Snowden revelations. Further, it can be difficult – if not highly subjective – to determine whether any given attack was intended for political or economic gain. On a global level, cyber espionage appears to be a silently accepted norm. The latest UN GGE (2015), for example, did not mention it in its latest publication, signalling that the international community is currently not motivated to address the topic, and its global curtailment, at least in the short term, is unlikely.

5 Conclusion

The Ukraine case study suggests that, during this conflict, nation-states have not adhered to many of the proposed 'political' cyber norms covered in this chapter. Hence, it is doubtful that these rules will be globally accepted in the near future.

43 See, for example, note 40 on 'The Cyberskeptics', and discussion between Jarno Limnéll and Thomas Rid. 'Is Cyberwar Real?,' *Foreign Affairs*, March/April 2014, https://www.foreignaffairs.com/articles/global-commons/2014-02-12/cyberwar-real.

44 See, for example, Martin Libicki. 'Would Deterrence in Cyberspace Work Even with Attribution?,' *Georgetown Journal of International Affairs*, April 22, 2015, http://journal.georgetown.edu/would-deterrence-in-cyberspace-work-even-with-attribution/.

45 Conversations with Ukrainian cyber security experts.

46 Brian Ries. 'Gang of Cyber Criminals on the Run in Ukraine and Russia,'*Mashable*, June 3, 2014, http://mashable.com/2014/06/03/cyber-criminals-russia-ukraine-gameover-zeus/; Tom Brewster. 'Trouble with Russia, Trouble with the Law: Inside Europe's Digital Crime Unit' *The Guardian*, April 15, 2014, http://www.theguardian.com/technology/2014/apr/15/european-cyber-crime-unit-russia.

First, the known cyber operations appear contrary to the letter and spirit of the Code of Conduct as most of the incidents can be seen as part of the larger information war. Second, most of the norms advocated by the US were also breached as cyber espionage was widely reported, and international cooperation between the two nation's CERTs and law enforcement agencies has been absent.

As a positive sign for international security, there have been no reports of destructive cyber attacks against CI in Ukraine. This appears to go against what one could expect to see in a modern military conflict. Is this a sign that the norm of not using cyber to harm CI – as also recently advocated by the UN GGE – is likely to be globally accepted and followed in the future? Hopefully, as this potential norm is perhaps the most important in terms of strengthening international cyber security and stability. As of October 2015, the Ukraine conflict appears to indicate that cyber operations have not yet (contrary to popular belief) substantially challenged the existing norms governing state behaviour in conflict situations.

Cyber operations have not yet (contrary to popular belief) substantially challenged the existing norms governing state behaviour in conflict situations.