A Legal Framework for Cyber Operations in Ukraine

by
Jan Stinissen

Chapter 14 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Lt Col Jan Stinissen of the NATO CCD COE, in Chapter 14, offers a legal framework for cyber operations in Ukraine. He explains that international law applies to cyberspace, and the law of armed conflict applies to all relevant cyber operations. Jan discusses the legal definitions of 'war' and 'cyberwar', as well as the concepts of 'armed conflict', 'armed attack', and 'use of force'. Typically, cyber attacks do not come in isolation, but rather as one element of a larger military operation; the wider context will determine the legal framework for its cyber component. There are many qualifying factors including state vs. non-state actor, and armed conflict vs. law enforcement. In the Ukraine crisis, operations in Crimea (which has already been annexed by Russia) may be viewed differently from those in eastern Ukraine. Stinissen asserts that, globally, most known cyber attacks have simply not been serious enough to be governed by the law of armed conflict, but that this is likely to change in the future.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

A Legal Framework for Cyber Operations in Ukraine

Jan Stinissen
NATO CCD COE

1 Introduction

Do the cyber attacks that we have seen during the Ukraine conflict constitute cyber-war? This chapter considers this question from a legal perspective. The term 'cyber-war' has no precise legal meaning. Even the term 'war' is less important than it used to be. Contemporary international law distinguishes 'armed conflict', 'armed attack', and 'use of force', but the question is how to place cyber conflict into that framework. In Ukraine, are we seeing 'cyber armed conflict' or merely cyber crime?

Cyber operations have to be considered within the context of the whole conflict. Although cyber can be used as stand-alone operation, the more likely case – and this holds true in Ukraine – is that cyber is used as a facilitator for other, more traditional types of warfare. The law applicable to the conflict as a whole should be applied to the cyber activities that are part of it. In other words, the wider context determines the legal framework for cyber operations. Particularly relevant is whether the conflict in Ukraine is an 'armed conflict' that leads to the application of the Law of Armed Conflict (or international humanitarian law).

This chapter will first briefly outline the applicability of international law to cyberspace. Then it will describe the legal framework of the conflict, related to the subsequent phases of the conflict, from the protests at Maidan Square in November 2013 to the present day. After that, the associated cyber activities will be placed in this legal context.

2 International Law and Cyber Operations

The applicability of international law to cyberspace has long been debated. Most Western countries posit that existing international law applies. Some countries, such as China and Russia, have proposed a unique and separate set of norms.[1] Today, it is generally recognised that international law applies, which is illustrated by the 2013 report of the Governmental Group of Experts, established by the United Nations (UN) General Assembly. It states that 'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'[2] However, the better question now concerns exactly *how* to apply international law in the cyber domain, and this is not a debate that will be resolved in the near future.[3] NATO 'recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace'.[4] It also considers cyber defence to be an intrinsic part of its collective defence task, and has declared that a cyber attack could have the impact as harmful as a conventional armed attack, which could lead to the invocation of Article 5 of the North Atlantic Treaty.[5]

In this chapter, the author takes as a premise that existing international law applies to cyberspace.

3 Legal Framework for the Conflict in Ukraine

Cyber activities conducted as part of a wider conflict are governed by that conflict's legal framework.

Cyber activities conducted as part of a wider conflict are governed by that conflict's legal framework. This section will describe the wider conflict in Ukraine. Section 1.4 will examine specific cyber incidents and how they fit into the larger legal puzzle.

1 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. An earlier version was submitted in September 2011.

2 United Nations, General Assembly, *Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98, 24 June 2013. The Group consisted of representatives of 15 nations, including the United States, Russia, and China. In their Report of July 2015, the GGE recommended a set of norms of behavior of states in cyberspace. For an analysis of this report, see Henry Rõigas and Tomáš Minárik. '2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law', *INCYDER database* , NATO CCD COE, 31 August 2015, https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html.

3 One of the prominent publications in this field is the *Tallinn Manual*. It discusses applicability of international law to cyber warfare, in particular the legal framework for the use of force and the law of armed conflict. The *Tallinn Manual* is prepared by an international group of experts on the invitation by the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia: Michael N. Schmitt, gen. ed., *Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013). Currently the *Manual* is under revision, a project coined *Tallinn 2.0*, including an analysis of international law applicable to cyber operations below the threshold of armed attack.

4 Wales Summit Declaration, 5 September 2014, para 72.

5 NATO's fundamental principle which states that 'if a NATO Ally is the victim of an armed attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked,' 'What is Article 5?', NATO, last updated 18 February 2005, http://www.nato.int/terrorism/five.htm.

3.1 Euromaidan (November 2013 – February 2014)

A few weeks before the European Union (EU) Eastern Partnership Summit in Vilnius, Lithuania, on 27-28 November 2013, during which the Ukraine – EU Association Agreement was to be signed, tensions in Ukraine were rising between those in favour and those opposed to closer relations with the EU. On 21 November, President Viktor Yanukovych decided to abandon the Association Agreement. This was followed by massive pro-EU demonstrations in *Maidan Nezalezhnosti* (Independence Square) in Kyiv. The clashes with the authorities grew violent. By mid-February, the events had escalated significantly, and had taken over 100 lives.

Before the *Euromaidan* protests began, tensions in Ukraine had already triggered hostile activity in cyberspace. Politically motivated hacker groups launched Distributed Denial-of-Service (DDoS) and other cyber attacks against a wide range of targets. On 28 October, the hacker group 'Anonymous Ukraine' started 'Operation Independence' (#OpIndependence), favouring Ukraine's independence from any external influence, including the EU, NATO, and Russia.[6] Operation Independence included DDoS attacks and website defacements against both Western and Russian sites. During *Euromaidan* DDoS attacks and defacements against both sides continued. Information leaks were used for propaganda purposes. Operation Independence leaked emails from opposition leader Vitali Klitchko and his political party, the Ukrainian Democratic Alliance for Reforms. Unknown hackers leaked the U.S. officials' phone call which included the infamous statement, 'f*ck the EU.'[7]

3.1.1 Legal Analysis

The *Euromaidan* protests were the violent culmination of a conflict between government authorities and pro-Western, civilian groups. Although the controversy was about Ukraine's external relations, it was primarily an internal matter between a state and an opposition within that state. And while the conflict engendered considerable violence – one only has to look at the number of casualties – at that stage, it could not be seen as an 'armed conflict'. It was not a conflict with 'armed forces on either side engaged in hostilities [...] similar to an international war'.[8] The incidents had the character of internal disturbances, civilian uprising, and violent clashes between protesters and police.

3.2 Forming Interim Government and Annexation of Crimea (February – March 2014)

On 21 February, President Yanukovych fled to Russia, and an Interim Government was formed, uniting the opposition. Events unfolded rapidly in Crimea. Pro-Russian gunmen seized key government buildings. On 1 March, the upper house of the Russian Parliament approved the deployment of troops in Ukraine to protect the

6 Eduard Kovacs. 'Anonymous Ukraine Launches OpIndependence, Attacks European Investment Bank', *Softpedia*, 31 October 2013, http://news.softpedia.com/news/Anonymous-Ukraine-Launches-OpIndependence-Attacks-European-Investment-Bank-395790.shtml.

7 Listen to recording here: https://www.youtube.com/watch?v=CL_GShyGv3o.

8 ICRC Commentary to Common Article 3 of the 1949 Geneva Conventions.

Russian speaking minority. Russian military forces (coined 'little green men') were reportedly present in Crimea and blocked the positions of Ukrainian troops.[9] A referendum, initiated by the Crimean Parliament, was held in Crimea on 16 March, which declared that 97% of voters supported joining Russia. Two days later, President Vladimir Putin signed a bill declaring Crimea to be part of the Russian Federation.[10] These events were crucial in setting the stage for the ongoing conflict in eastern Ukraine, and led to a dramatic change in relations between Russia and the West.

In cyberspace, there was a simultaneous rise in malicious activity during the military operations in Crimea. Operations were conducted against Ukraine's mobile infrastructure, the mobile phones of members of the Ukrainian Parliament, and security communications. Some traditional methods were used, including the seizure of *Ukrtelecom* offices and the physical cutting of telephone and internet cables.[11] Digital attacks included DDoS targeting Ukrainian, Crimean, NATO, and Russian websites. The pro-Russian hacker group *CyberBerkut* was particularly active against NATO,[12] while groups like *OpRussia* and *Russian CyberCommand* directed their actions against Russian websites.[13] Polish, Ukrainian, and Russian websites were also defaced, including the site of *Russia Today*, sometimes with historical references to World War II.[14]

Information leaks continued. A sensitive conversation between the Estonian Minister of Foreign Affairs Urmas Paet and EU High Representative for Foreign Affairs and Security Policy Catherine Ashton was made public, revealing their discussion of information suggesting that both sides, the opposition *and* the government, were responsible for sniper killings during the Maidan protests.[15] Anti-Russian motivated information leaks included the disclosure of the names of members of *Berkut*, the anti-riot police,[16] as well as documents belonging to a Russian defence contractor.[17]

During this time, it also became clear that the spyware *Snake* (also known as *Ouruborus* or *Turla*) was used against several targets in Ukraine, including the government. *Snake* is sophisticated malware, known to be in use for at least eight years, whose origin is uncertain, but believed to be developed in Russia.[18]

9 Vitaly Shevchenko. '"Little green men" or "Russian invaders"?', *BBC News*, 11 March 2014, http://www.bbc.com/news/world-europe-26532154.

10 See for an overview of events: 'Ukraine crisis: timeline', *BBC News*, http://www.bbc.com/news/world-middle-east-26248275.

11 John Leyden. 'Battle apparently under way in Russia-Ukraine conflict', *The Register*, 4 March 2014, http://www.theregister.co.uk/2014/03/04/ukraine_cyber_conflict/.

12 Adrian Croft and Peter Apps. 'NATO websites hit in cyber attack linked to Crimea tension', *Reuters*, 16 March 2014, http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316.

13 Jeffrey Carr. 'Rival hackers fighting proxy war over Crimea', *Reuters*, 25 March 2014, http://edition.cnn.com/2014/03/25/opinion/crimea-cyber-war/. Contrary to what its name suggests, *Russian CyberCommand* is a hacker group acting *against* Russian authorities.

14 Darlene Storm. 'Political hackers attack Russia, Nazi defacement, threaten US CENTCOM with cyberattack', *Computerworld*, 3 March 2014, http://www.computerworld.com/article/2476002/cybercrime-hacking/political-hackers-attack-russia--nazi-defacement--threaten-us-centcom-with-cybera.html.

15 Ewen MacAskill. 'Ukraine crisis: bugged call reveals conspiracy theory about Kiev snipers', *The Guardian*, 5 March 2014, http://www.theguardian.com/world/2014/mar/05/ukraine-bugged-call-catherine-ashton-urmas-paet.

16 Jeremy Bender. 'EXPERT: The Ukraine-Russia Cyberwar Is 'More Serious And Damaging' Than The Annexation Of Crimea', *Business Insider*, 10 March 2014, http://www.businessinsider.com/ukraine-russia-cyberwar-extremely-serious-2014-3.

17 Bindiya Thomas. 'Rosoboronexport Denies Loss of Confidential Data in Cyber Attack', *Defense World.net*, 25 March 2014, http://www.defenseworld.net/news/10275/Rosoboronexport_Denies_Loss_of_Confidential_Data_in_Cyber_Attack#.VbzA8fmMCXQ.

18 Sam Jones. 'Cyber Snake plagues Ukraine networks', *Financial Times*, 7 March 2014, http://www.ft.com/cms/s/0/615c29ba-a614-11e3-8a2a-00144feab7de.html#axzz3gDUpc1wz.

3.2.1 Legal Analysis

Although the UN and EU expressed their grave concerns about Russia's annexation of Crimea, and NATO called it a violation of international law,[19] Russia defended its actions as the lawful protection of the Russian speaking minority in Crimea. States have the right to act when necessary to rescue their nationals abroad. However, in this case, there were no indications that native Russians were in danger. Even if that were the case, it could only have justified their evacuation, *not* the occupation of the entire peninsula.[20] A second possible justification for Russian intervention was an invitation by the Ukrainian authorities, i.e. President Yanukovych. But, after Yanukovych was replaced by the Interim Government, his actions could not be attributed to Ukraine anymore.[21] A third possible justification is the right to self-determination for the people of Crimea. However, while this right exists for 'peoples' within the existing borders of a state, it does not allow for a complete political separation.[22]

Russia's annexation of Crimea was a breach of international law by violating the territorial integrity of Ukraine. Russia also breached the 1994 Budapest Memorandum and the 1997 Treaty on Friendship, Cooperation, and Partnership.[23] The Black Sea Fleet Status of Forces Agreement allowed for a Russian military presence in Crimea, but not at the scale as was the case in March 2014. But was this armed intervention also a use of force, a violation of Article 2(4) of the UN Charter?[24] Moving armed forces to the territory of another state, without the consent of that state, should definitely be considered a use of force.[25] That is exactly what happened: troops belonging to the Russian Black Sea Fleet in Crimea left their bases, and there were clear indications that other Russian

> *Russia's annexation of Crimea was a breach of international law.*

19 '[A] spokesman for UN Secretary-General Ban Ki-moon delivered a statement saying that he was 'gravely concerned about the deterioration of the situation' in Ukraine and planned to speak shortly with Putin. It also called for 'full respect for and preservation of the independence, sovereignty and territorial integrity of Ukraine' and demanded 'immediate restoration of calm and direct dialogue between all concerned'. Representative of the Union for Foreign Affairs and Security Policy Catherine Ashton stated that the EU "deplores" what it called Russia's decision to use military action in Ukraine, describing it as an "unwarranted escalation of tensions". She called on "all sides to decrease the tensions immediately through dialogue, in full respect of Ukrainian and international law". She added that: 'The unity, sovereignty and territorial integrity of Ukraine must be respected at all times and by all sides. Any violation of these principles is unacceptable'. North Atlantic Council condemned what it called Russia's military escalation in Crimea and called it a breach of international law'. International reactions to the annexation of Crimea by the Russian Federation, Wikipedia, accessed 1 August 2015, https://en.wikipedia.org/wiki/International_reactions_to_the_annexation_of_Crimea_by_the_Russian_Federation.

20 See also: Marc Weller, in BBC News, 'Analysis: Why Russia's Crimea move fails legal test', *BBC News*, 7 March 2014, http://www.bbc.com/news/world-europe-26481423.

21 See also: Christian Marxsen, 'The Crimea Crisis – An International Law Perspective,' *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (Heidelberg Journal of International Law)* 74/2 (2014): 367-391; Remy Jorritsma. 'Ukraine Insta-Symposium: Certain (Para-)Military Activities in the Crimea: Legal Consequences for the Application of International Humanitarian Law', *Opinio Juris*, 9 March 2014, http://opiniojuris.org/2014/03/09/ukraine-insta-symposium-certain-para-military-activities-crimea-legal-consequences-application-international-humanitarian-law/; Ashley Deeks. 'Here's What International Law Says About Russia's Intervention in Ukraine', *New Republic*, 2 March 2014, http://www.newrepublic.com/article/116819/international-law-russias-ukraine-intervention.

22 Marxsen. 'Crimea Crisis,' 14; Jorritsma. 'Legal Consequences.'

23 The 1994 Budapest memorandum was intended to provide Ukraine security in exchange of accession to the Treaty on the Non-Proliferation of Nuclear Weapons. Russia, the United States, and the United Kingdom committed to 'respect the independence and sovereignty and the existing borders of Ukraine'. The 1997 Treaty on Friendship, Cooperation, and Partnership between Russia and Ukraine was to guarantee the inviolability of the borders between both states. See also: Marxsen, 'Crimea Crisis,' 4-5.

24 Charter of the United Nations, San Francisco, 26 June 1945, Article 2(4).

25 See also: Deeks. 'What International Law Says.'

troops were sent to Crimea to secure strategic sites, block Ukrainian troops, and essentially force them to leave the peninsula.

States can take measures in response to violations of international law. In this case the European Union and the United States imposed sanctions on Russia.

Could Russia's actions be seen as an armed attack, in which case Ukraine would have had the right to use force in self-defence?[26] Like 'use of force', 'armed attack' is not defined in the UN Charter; in essence, a state determines on a case-by-case basis whether it considers an attack against it as an 'armed attack'. A violent attack with military forces resulting in damage and casualties would certainly be seen as an armed attack. In the case of Crimea, however, hardly a shot was fired. On the other hand, it is difficult to argue that Ukraine would *not* have the right to use force to drive Russian troops out of Crimea.[27]

Irrespective this analysis of the *legal basis* of the intervention in Crimea, what would be the *legal regime* for the operations conducted by the parties to the conflict, including the cyber operations? Did the situation qualify as an 'international armed conflict' where the Law of Armed Conflict applies? The criterion here is that it relates to hostilities between nation-states. In Crimea, however, the situation was unclear. Firstly, there was no fighting, although the threshold for 'armed' is low.[28] Secondly, Russia denied the troops present were theirs and referred to them as 'local self-defence groups'. However, reports indicated the active involvement of Russian troops[29] and, eventually, Putin admitted that Russian troops were present.[30] Even in the event that only local forces were active, a situation of international armed conflict could still prevail if they were acting under Russia's control.

> *The Law of Armed Conflict applies in a situation of total or partial occupation.*

The Law of Armed Conflict also applies in a situation of a total or partial occupation, even if the occupation did not meet armed resistance.[31] Occupation is a 'hostile substitution of territorial power and authority'.[32] This is precisely the case in Crimea, where Russia exercises territorial control without the consent of the Ukrainian Government.

26 Charter of the United Nations, Article 51.

27 Deeks. 'What International Law Says.'

28 'Any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place. The respect due to the human person as such is not measured by the number of victims', ICRC Commentary to the Geneva Conventions of 1949, 20-21.

29 For example: 'Ukrainian and Russian troops in standoff at Crimean military base – As it happened', *The Guardian*, 3 March 2014, http://www.theguardian.com/world/2014/mar/02/ukraine-warns-russia-crimea-war-live; and 'Russian troops storm Ukrainian bases in Crimea', *BBC News*, 22 March 2014, http://www.bbc.com/news/world-europe-26698754

30 'Putin Admits Russian Troop Role in Crimea Annexation', *Voice of America*, 17 November 2014, http://www.voanews.com/content/putin-admits-russian-troop-role-in-crimea-annexation/2523186.html; 'Putin admits Russian forces were deployed to Crimea', Reuters, 17 April 2014, http://uk.reuters.com/article/2014/04/17/russia-putin-crimea-idUKL6N0N921H20140417.

31 Geneva Conventions, 12 August 1949, Common Article 2.

32 Hague Regulations: Regulations concerning the Laws and Customs of War on Land, 18 October 1907, Article 42. See also: Jorritsma, 'Legal Consequences.'

3.3 Hostilities in Eastern Ukraine (April 2014 – Present)

Following the annexation of Crimea, the world's attention was quickly drawn to the onset of hostilities in eastern Ukraine. Protesters from the Russian speaking minority in the cities of Donetsk, Luhansk, and Kharkiv occupied government buildings and called for independence.[33] Pro-Russian 'separatist groups' emerged. The Ukrainian authorities responded by starting an 'anti-terrorist operation'. On 17 April, the first violent deaths occurred in eastern Ukraine; in the Black Sea city of Odessa, 42 people died in clashes. On 11 May, Donetsk and Luhansk declared themselves to be independent republics.

Petro Poroshenko was elected President of Ukraine on 25 May, but this poll could not be held in large parts of the conflict-ridden east. A cease-fire agreement,[34] signed in Minsk on 5 September 2014, collapsed when fighting started again in January 2015. A second agreement signed in the capital of Belarus on 11 February, *Minsk II*, provided for a ceasefire, the withdrawal of heavy weapons from the front line, a release of prisoners of war, and constitutional reform in Ukraine.[35] This second agreement has also been violated, although currently, in September 2015, the situation seems to have calmed down. NATO reported the active involvement of Russian troops in eastern Ukraine,[36] but Russia has consistently denied involvement.

Cyber operations have continued throughout the conflict. In May 2014, cyber means were used in an attempt to disrupt the presidential elections, including an effort to falsify the outcome. *CyberBerkut* may have taken part and some analysts believe that Russia was behind it.[37] In August 2014, hackers conducted a DDoS attack against Ukraine's election commission website, just prior to the parliamentary polls.[38]

There are numerous publicly-known examples of intelligence gathering through cyber means, all of which reportedly have a Russian connection. In the Summer of 2014, the *Blackenergy* spyware was used against Ukrainian government institutions.[39] In August, the *Snake* malware was employed against the Ukrainian Prime Minister's Office, as well as a number of foreign embassies.[40] In April 2015, *Lookinglass* reported on a Russian campaign to extract classified documents from Ukrainian military and law enforcement agencies in an effort to support pro-Russian military

33 'Ukraine crisis: Timeline', *BBC News*, accessed 1 August 2015, http://www.bbc.com/news/world-middle-east-26248275.

34 Protocol on the results of consultations of the Trilateral Contact Group, Minsk, 5 September 2014, http://mfa.gov.ua/en/news-feeds/foreign-offices-news/27596-protocolon-the-results-of-consultations-of-the-trilateral-contact-group-minsk-05092014.

35 'Ukraine ceasefire: New Minsk agreement key points', *BBC News*, 12 February 2015, http://www.bbc.com/news/world-europe-31436513.

36 See for example: 'NATO Commander: 'Conditions in Eastern Ukraine Have to Change", OPB, 6 February 2015, http://www.opb.org/news/article/npr-nato-commander-conditions-in-eastern-ukraine-have-to-change/, and 'Nato urges Russia to stop fuelling Ukraine conflict', *The Irish Times*, 15 April 2015, http://www.irishtimes.com/news/world/europe/nato-urges-russia-to-stop-fuelling-ukraine-conflict-1.2176718.

37 Mark Clayton. 'Ukraine election narrowly avoided 'wanton destruction' from hackers (+video)', *The Christian Science Monitor*, 17 June 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

38 'Hackers attack Ukraine election website', *Presstv*, 25 October 2014, http://www.presstv.ir/detail/2014/10/25/383623/ukraines-election-website-hacked/. See also: Vitaly Shevchenko, 'Ukraine conflict: Hackers take sides in virtual war', BBC News, 20 December 2014, http://www.bbc.com/news/world-europe-30453069.

39 David Gilbert. 'BlackEnergy Cyber Attacks Against Ukrainian Government Linked to Russia', *International Business Times*, 26 September 2014, http://www.ibtimes.co.uk/blackenergy-cyber-attacks-against-ukrainian-governm)ent-linked-russia-1467401.

40 Sam Jones. 'Russia-linked cyber attack on Ukraine PM's office', *CNBC*, 8 August 2014, http://www.cnbc.com/id/101905588.

operations in Ukraine.[41] *ISight Partners* reported that Russian *Sandworm* hackers used a 'zero-day' vulnerability to hack NATO and Ukraine in a cyber espionage campaign.[42] The list of targets was not confined to Ukrainian sites. In January 2015, *CyberBerkut* claimed responsibility for a cyber attack on German Government sites, demanding that Germany end its support to the Ukrainian government.[43]

On the pro-Ukraine side, the *Ukrainian Cyber Troops* reportedly claimed to have hacked into Russian interior ministry servers and CCTV cameras in separatist-controlled eastern Ukraine.[44]

3.3.1 Legal Analysis

The International Committee of the Red Cross (ICRC) has characterised the situation in eastern Ukraine as a 'non-international armed conflict',[45] a situation in which hostilities occur between governmental armed forces and non-governmental organised armed groups, or between such organised armed groups. The two requirements are a certain degree of organisation of the non-governmental groups and the existence of 'protracted armed violence'.[46] The conflict in Eastern Ukraine does in fact reach a high level of violence over a longer period of time, and the separatists do in fact have a high degree of organisation.

Although Russia has consistently denied involvement, there continues to be widespread belief to the contrary, suggesting that Moscow actively supports the Donetsk and Luhansk separatists, including by sending Russian military forces as 'volunteers' to the area. If Russia actively participates or exercises 'overall control' over the separatists, the conflict could be considered an international armed conflict. To meet the criterion of 'overall control', a state must not only finance, train, equip, or provide operational support to local forces, but also have a role in organising, coordinating, and planning their operations.[47]

However, for the purpose of this chapter, the conflict in eastern Ukraine is considered to be a non-international armed conflict.

This analysis results in a situation where different legal regimes apply simultane-

41 Aarti Shahani. 'Report: To Aid Combat, Russia Wages Cyberwar Against Ukraine', *NPR*, 28 April 2015, http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine.

42 Ellen Nakashima. 'Russian hackers use 'zero-day' to hack NATO, Ukraine in cyber-spy campaign', *The Washington Post*, 13 October 2014, http://www.washingtonpost.com/world/national-security/russian-hackers-use-zero-day-to-hack-nato-ukraine-in-cyber-spy-campaign/2014/10/13/f2452976-52f9-11e4-892e-602188e70e9c_story.html.

43 Michelle Martin and Erik Kirschbaum. 'Pro-Russian group claims cyber attack on German government websites', *Reuters*, 7 January 2015, http://www.reuters.com/article/2015/01/07/us-germany-cyberattack-idUSKBN0KG15320150107.

44 'The Daily Beast: Ukraine's lonely cyber warrior,' *KyivPost*, 18 February 2015, http://www.kyivpost.com/content/ukraine-abroad/the-daily-beast-ukraines-lonely-cyber-warrior-381094.html, and Vitaly Shevchenko, 'Ukraine conflict: Hackers take sides in virtual war', BBC News, 20 December 2014, http://www.bbc.com/news/world-europe-30453069.

45 'Fighting in eastern Ukraine continues to take its toll on civilians, and we urge all sides to comply with international humanitarian law, otherwise known as the law of armed conflict', said Mr Stillhart. 'These rules and principles apply to all parties to the non-international armed conflict in Ukraine, and impose restrictions on the means and methods of warfare that they may use [in Ukraine]': ICRC calls on all sides to respect international humanitarian law, *ICRC News Release* 14/125, 23 July 2014. Non-international armed conflicts are 'armed conflicts not of an international character occurring in the territory of one of the High Contracting Parties,' Geneva Conventions, Common Article 3.

46 The criterion 'protracted armed violence' stems from Tadić, Decision on the Defence Motion for Interlocutory Appeal, para 70, International Criminal Tribunal for the Former Yugoslavia, 2 October 1995.

47 'Overall control' is addressed in: Tadić, Appeals Chamber judgment, International Criminal Tribunal for the Former Yugoslavia, 15 July 1999, para 132, 137, 141, and 145. See also: *Tallinn Manual*, 79-82.

ously. The Law of Armed Conflict pursuant to international armed conflicts applies to the occupation of Crimea. Eastern Ukraine is a national issue in which the law pursuant to *non*-international armed conflicts applies. There is a crucial difference. During an international armed conflict, the Law of Armed Conflict applies to the full extent; during a non-international armed conflict, minimum rules apply.[48] An example is that in an international armed conflict, combatants captured by the enemy are entitled to Prisoner of War (PoW) status. In a non-international armed conflict, the combatant's status is unknown; belligerents have to be treated well, but the extensive rules that protect PoWs do not apply. However, many rules of international armed conflict are customary law and apply also in a non-international armed conflict, as we will see with respect to cyber operations.

4 Legal Implications for Cyber Operations in Ukraine

The conflict started as an internal matter, the protests at Maidan Square, to an unlawful intervention and occupation of Crimea, culminating in the non-international armed conflict in eastern Ukraine.

During the first phase, the *Euromaidan* protests, the cyber incidents were a law enforcement issue. For example, the defacement of websites and DDoS attacks restricting the use of internet services violated Ukrainian criminal law and could have been prosecuted in Ukrainian courts.[49] Malicious cross-border cyber activities, involving both Ukraine and other countries, would fall under the criminal jurisdiction of Ukraine and the affected countries.

During the occupation of Crimea and the armed conflict in eastern Ukraine, the Law of Armed Conflict applies. It regulates the conduct of all actors in the conflict, including the cyber actors. Hereafter, first the status of the different cyber actors will be discussed; after that the cyber operations we have seen in the Ukraine conflict will be evaluated from the perspective of the Law of Armed Conflict.

> *During the Euromaidan protests, cyber incidents were a law enforcement issue.*

4.1 Actors in Cyberspace

In an *international* armed conflict, belligerents that qualify as 'combatants' enjoy combatant immunity, meaning they cannot be prosecuted for taking part in hostilities (except

48 These 'minimum rules' are formulated in Common Article 3 of the Geneva Conventions, and in Additional Protocol II to the Geneva Conventions. The rules laid down in that protocol apply to a conflict within a state that is party to the Protocol between the armed forces of that state and dissident armed forces or organised armed groups that control sufficient territory so 'as to enable them to carry out sustained and concerted military operations', Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, Article 1(1). Ukraine is party to Additional Protocol II, and the separatists do control significant territory.

49 Ukraine is Party to the Convention on Cybercrime (Budapest, 2001). The Convention aims to harmonise cybercrime legislation and facilitate information exchange and international cooperation in the area of prosecution of cybercrimes. States that are party to the convention are obliged to incorporate certain violations in their national laws: 'illegal access', 'illegal interception', 'data interference', 'system interference', and 'misuse of devices'.

for war crimes) and, on capture, have PoW status. These rules also apply during occupation, as in Crimea. Most cyber actors in Crimea were nominally non-state actors, for example the pro-Russian hacker group *CyberBerkut*. If such a group were an integrated part of Russia's military forces, they would be combatants. If not, they could nevertheless be considered combatants if they were part of an organised armed group, belonging to a party to the conflict, when they fulfil the following conditions: (a) being commanded by a person responsible for his subordinates; (b) having a fixed distinctive sign recognisable at a distance; (c) carrying arms openly; and (d) conducting their operations in accordance with the laws and customs of war.[50] These criteria are important to distinguish combatants from civilians. It is unlikely that non-state hacker groups, also those active in the Ukraine crisis, meet all these criteria, especially when they are only 'virtually' organised, only in contact through the internet.

Hackers or hacker groups who are non-combatants are to be regarded civilians. However, if they are 'directly participating in hostilities', they lose their protection as civilians and can be targeted by the opposing party. Three criteria have to be met to be regarded 'civilians directly participating in hostilities.'[51] First, there has to be a certain amount of 'harm'; the 'act must be likely to adversely affect the military operations or military capacity of [the adversary] or […] to inflict death, injury or destruction on persons or objects protected against direct attack'.[52] Second, there has to be a 'causal connexion' between the acts and the harm inflicted. Third, there has to be a 'belligerent nexus', meaning that the operations must be intended to affect the adversary's military operations. Harm can also be inflicted by cyber operations, and does not necessarily have to include physical damage. In the case of *CyberBerkut* and other active hacker groups the effects probably did not reach the threshold of 'harm'.

In *non-international* armed conflicts, like in eastern Ukraine, 'combatant immunity' does not exist. Whether or not belligerents – especially non-state armed groups – have immunity, will be determined based on domestic law. Certain cyber operations will be illegal based on domestic law. Civilians have protected status, but as in international armed conflicts, when they are 'directly participating in hostilities' they lose that protected status.

4.2 Information Operations

During the conflict in Ukraine, cyber was mainly used for information warfare and intelligence gathering – not to damage cyber or critical infrastructure. Irrespective their effects, cyber operations are very often called 'cyber attack.' It is important to note that, in the context of international and non-international armed conflicts, 'attack' has a very specific meaning. 'Attacks means acts of violence against the adversary, whether in offence or in defence.'[53] Whether or not an operation qualifies as attack is crucial

50 Geneva Convention (III), 12 August 1949, Article 4, para A(2).
51 ICRC Interpretive guidance on the notion of Direct Participation in hostilities under international humanitarian law, May 2009.
52 ICRC Interpretive guidance, 47.
53 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 49(1).

because the law imposes prohibitions and restrictions with respect to attacks, for example the prohibition to attack civilians, civilian objects, and medical installations, and the requirement to take precautions before conducting an attack. Not every cyber operation that affects the adversary is an attack. A cyber operation that constitutes an act of violence however, *is* an attack. The *Tallinn Manual* defines a 'cyber attack' as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.'[54] This interpretation of the current law restricts 'cyber attacks' to acts that have physical consequences.

If the parties to the conflict in Ukraine would have used cyber to inflict physical damage, injuries, or death, or to support kinetic operations, those cyber operations would be '(cyber) attacks' and subject to the relevant prohibitions and restrictions. Most of the cyber activities in Ukraine however are information operations and do not meet the 'attack' threshold. Information operations, as such, are not directly addressed in the Law of Armed Conflict. Whether they would be in violation of the law basically depends on the content of the message. One example would be disseminating a threatening message with the purpose to spread terror among the civilian population.[55] The disruption of elections, that took place in Ukraine, definitely violated domestic law, and when conducted or supported by another state, could also have been a breach of international law, but was not a violation of the Law of Armed Conflict.

Information operations, as such, are not directly addressed in the Law of Armed Conflict.

4.3 Cyber Espionage

During the conflict in Ukraine, cyber means have been used to gather intelligence including *Snake*, *Blackenergy*, and *Sandworm*. Intelligence gathering and espionage are not forbidden by international law. Espionage, in the context of the Law of Armed Conflict, has a narrow scope: it refers to operations that are conducted clandestinely or under false pretences, taking place on territory controlled by the adversary; 'behind enemy lines'.[56] For instance, a close access cyber operation where an agent is gaining access to servers being used by the adversary by feigning a false identity and extracting information by using a thumb drive, could be espionage. An agent captured before reaching his own troops has no PoW status and can be tried as a spy. Gathering intelligence from a distance is not espionage in the meaning of the Law of Armed Conflict.

Snake, *Blackenergy*, and *Sandworm* reportedly have a Russian connection. If Russia – or another state – would be actively supporting the separatists in eastern Ukraine by providing intelligence, that would not necessarily 'internationalise' the conflict. Mere operational support does not meet the 'overall control' threshold.[57]

54 *Tallinn Manual*, 106.
55 Protocol I, Article 51(2), and Protocol II, Article 13(2).
56 *Tallinn Manual*, 192-193.
57 *Tallinn Manual*, 81.

5 Conclusions

International law applies to cyberspace. During armed conflict, the Law of Armed Conflict applies to any cyber operation conducted in association with the hostilities. Until now, we have not seen a case where cyber hostilities between parties *by themselves* constituted an armed conflict. Rather, they have remained as one part of a larger, traditional conflict. This dynamic has not changed during the conflict in Ukraine.

This chapter describes the international legal framework for the conflict in Ukraine and the cyber operations that have been conducted in association with that conflict. The 'legal situation' is somewhat unclear due to diverging views on various aspects of the crisis, such as the annexation of Crimea and the alleged involvement of Russian military forces in eastern Ukraine. Another aspect that complicates a legal evaluation is that cyber operations are often conducted by non-state actors, whose status and affiliation are not always clear.

The protests at Maidan Square turned violent, but they were not an 'armed conflict'; they were an internal law enforcement matter. The annexation of Crimea led to the peninsula's occupation by Russia, but Russia disputes that interpretation. During an occupation, the Law of Armed Conflict applies. Eastern Ukraine can today be considered a non-international armed conflict, where cyber operations must be conducted in accordance with the minimum safeguards the Law of Armed Conflict provides for such situations.

> *Cyber operations are often conducted by non-state actors, whose status and affiliation are not always clear.*

In the Ukraine conflict, the publicly known cyber operations have not generally been considered to be sophisticated – likely not corresponding to the real national capabilities of Russia and Ukraine. The prevailing assumption is that, with the exception of some advanced cyber espionage malware such as Snake, the known cyber attacks could have been conducted by non-state actors. These hackers or hacker groups, trying to affect the adversary's military activities, are participating in hostilities and have to conduct their operations in accordance with the Law of Armed Conflict.

At the end of the day, cyber operations in the Ukraine conflict have been used either to gather intelligence or as part of an ongoing 'information war' between the parties. They were not launched to inflict damage to infrastructure and other military capabilities. As a result, most of these cyber operations have not yet risen to the level of activities proscribed or even governed by the Law of Armed Conflict. That would be different when cyber would be more integrated in kinetic warfare operations.