2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Cyber Weapons Review in Situations Below the Threshold of Armed Conflict

Ivana Kudláčková*
Researcher
Faculty of Law
Masaryk University
Brno, Czech Republic
ivana.kudlackova@law.muni.cz

David Wallace
Professor
Department of Law
United States Military Academy
West Point, New York, US
david.wallace@westpoint.edu

Jakub Harašta*
Assistant Professor
Faculty of Law
Masaryk University
Brno, Czech Republic
jakub.harasta@law.muni.cz

Abstract: The use of cyber weapons raises many issues, one of which is the scope of legal requirements affecting the legal review of cyber weapons under Additional Protocol I and customary international law. This paper explores the review of cyber weapons intended for use below the threshold of armed conflict

As the line between war and peace is often increasingly blurred and the majority of cyber incidents are below the threshold of armed conflict, the laws and principles of international humanitarian law do not apply. In this paper, we engage in a scenario-based thought experiment exploring the legal framework affecting the use of cyber weapons outside armed conflict. In such situations, the well-known article 36 of Additional Protocol I and customary international law are not triggered. As a result, there is no explicit legal obligation to conduct a cyber weapons review in situations when cyber weapons are deployed in situations falling below the threshold of armed

* Ivana Kudláčková's and Jakub Harašta's contributions to this paper were supported by ERDF 'CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence' (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

conflict. Our starting point is that even though international humanitarian law is not applicable, the use of cyber weapons is not completely unregulated.

In the paper, we search for answer to following research question: what are the legal requirements for weapons review in situations where their intended use is for situations below the threshold of armed conflict? We identify the black-letter legal framework and explore the state practice of NATO member states where available.

The paper argues that there are many obligations to be considered when deploying cyber weapons in situations below the threshold of armed conflict. The conclusion is that there is no obligation to conduct a review outside Article 36 of Additional Protocol I. That being said, there are definitely policy benefits in conducting broader software assessment to ensure respect to international law obligations of a state.

Keywords: *cyber weapons, software, legal review, art. 36 of Additional Protocol I, human rights*

1. INTRODUCTION

The regulation of cyber weapons under international law has been an unsettled issue, not only among international lawyers but also among information technology specialists and political and security researchers. This uncertainty presents a challenge to reconsider the existing norms of international law, especially the obligation to conduct a weapons review imposed by Article 36 of Additional Protocol I (API) and customary international law. Legal review of cyber weapons has been already discussed in, amongst other places, the *Tallinn Manual 2.0* and the Cyber Law Toolkit. Understandably, both focused on the weapons review requirement under international humanitarian law (IHL). In our opinion, however, this approach does not fully reflect the cyber reality. In this paper, we explore the issue of weapons review beyond Article 36 of API and examine other possible legal regimes to account for legal requirements that appear elsewhere in the conflict classification framework.[1]

This paper seeks to answer the following research question:

What legal requirements need to be considered when deploying cyber weapon in situations below the threshold of armed conflict?

1 Compare David A. Wallace and Christopher W. Jacobs, 'Conflict Classification and Cyber Operations: Gaps, Ambiguities and Fault Lines', (2019) 40 *U. Pa. J. Int'l L*, 643.

The paper is structured as follows. First, we encapsulate existing definitional approaches to cyber weapons and introduce our working definition. Second, we present a hypothetical scenario with escalating conflict between two fictional States – scenario contains both cyber and non-cyber events that drive escalation towards armed conflict. Third, these incidents are explored through the lens of various legal regimes, such as derogation of human rights, issues of sovereignty and non-intervention, and the use of force, armed attack and armed conflict. Finally, we discuss the existing connection between limits imposed on the use of cyber weapons by international public law in general, hence reaching beyond the narrow scope of Article 36 of API.

2. CYBER WEAPONS: WORKING DEFINITION AND WEAPONS REVIEW

A. Cyber Weapons

Given the various technical, legal, security and policy aspects of the term *cyber weapons*, it is highly unlikely that a universally accepted definition will ever be reached. That being said, reaching at least a working definition makes the issue more accessible for discussion. The term *weapon* carries normative meaning pointing us directly to Article 36 of API. Automatically, it triggers the requirement to conduct a formalised weapon review. Therefore, we use the term software for scenarios below the threshold of armed conflict and we reserve the term cyber weapon only for the context of international armed conflict. Our decision directly stems from the wording used in Rule 103 of the *Tallinn Manual 2.0* and from some of the works mentioned below.

Generally, scholars trying to define cyber weapons follow two trends. The first group focuses on the intended target of the cyber weapon and on its ability to cause damage.[2] Damage is crucial here, as some authors acknowledge that without the ability to cause damage, even highly invasive techniques such as data exfiltration do not constitute a cyber weapon.[3] We are proponents of the concept that data is an object and might be qualified as a military objective.[4] However, we recognise that this is a very controversial and unsettled issue. The second group simply refers to cyber incidents without really intending to provide a clear definition of the term cyber weapon. Some authors mention Stuxnet, the DDoS attacks on Estonia in 2007 or the use of

2 Peeter, Lorents and Rain Ottis, 'Knowledge Based Framework for Cyber Weapons and Conflict', (2010) *Conference on Cyber Conflict Proceedings* 129, 139. Amit. K. Maitra, 'Offensive cyber-weapons: technical, legal, and strategic aspects', (2015) 35 *Environment Systems and Decisions* 169, 179. Thomas Rid and Peter McBurney, 'Cyber-Weapons', (2012) 157 *The RUSI Journal* 6, 7.

3 Jacqueline Eggenschwiller and Jantje Silomon, 'Challenges and opportunities in cyber weapon norm construction', (2018) 12 *Computer Fraud & Security* 11, 12. Sami Zhioua, 'The Middle East under Malware Attack Dissecting Cyber Weapons', (2013) *IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings* 11, 11.

4 Compare Kubo Mačák. 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law', (2015) 48 *Israel Law Review* 55.

the malware Shamoon against Saudi Aramco in the same breath.[5] If those incidents are not followed by in-depth analysis with an aspiration towards understanding the term cyber weapon and its normative consequences, it presents a threat of undesirable simplification that floods the issue of cyber security.

The International Group of Experts (IGE) drafting the *Tallinn Manual 2.0* dedicated Rule 103 not only to weapons, but also more broadly to means and methods of cyber warfare in general. Cyber weapons are understood to be 'cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of persons or damage to, or destruction of 'objects'.[6] Furthermore, the IGE distinguished between cyber weapons and cyber systems. A weapon is one of the aspects of a cyber system and is used to 'cause damage or destruction to objects or injury or death to persons'.[7] Given the scope and aim of the *Tallinn Manual 2.0*, these definitions stem mainly from IHL and reflect predominantly Article 36 of API. The definition of cyber weapons is thus closely tied to that of the cyber attack in Rule 92 of the *Tallinn Manual 2.0*. In this view, cyber weapons are intended to execute cyber attacks.

However, as the nature of interstate interaction and possible conflicts evolve, we believe broader considerations are in place. Cyber systems can be used to deliver harmful software to targeted systems. Different payloads can lead to different harmful consequences. However, these consequences may not be so dire as to justify the use of the term 'weapon'; indeed, we believe the current over-use of the term cyber weapon is harmful and obfuscates the discussion. Hence, we take into consideration the cyber systems used to deliver harmful software. Some of the harmful software may ultimately be labelled a cyber weapon. We believe this allows for a more nuanced discussion regarding the existing legal requirements and respects that weapon is just an aspect of a cyber system.[8] As is evident from Figure 1, cyber systems can be used to deliver software into particular targeted devices (different payloads) and only some payloads can be considered cyber weapons. Cyber systems are made up of general infrastructure (operators, means of payload delivery, command and control servers) and additional payloads serving specific purposes. The effects of these payloads may or may not have physical consequences. Some of these payloads may be considered cyber weapons under existing law. However, elucidation of the exact nature of those consequences is not the purpose of this paper. In Figure 1, we do not aspire to provide a universal scheme, but rather to suggest that some sort of a review needs to be conducted, not only in case of use of cyber weapons, but also in case of use of harmful software.

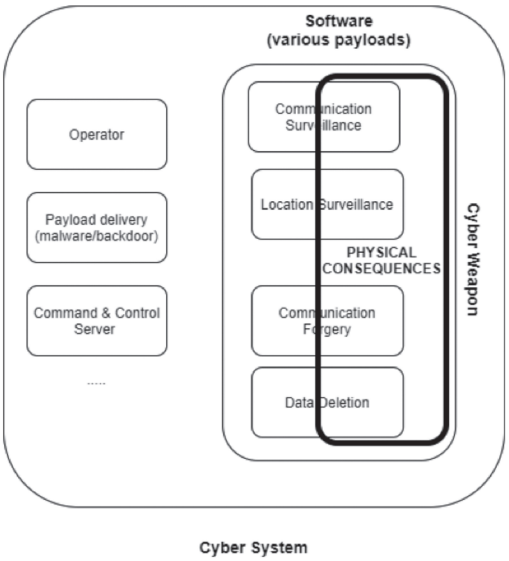
5 Ivanka Barzaszka, 'Are cyber-weapons effective?' (2013) 158 *The RUSI Journal* 48, 48. Gregory D. Koblentz and Brian M. Mazanec, 'Viral Warfare: The Security Implications of Cyber and Biological Weapons', (2013) 32 Comparative Strategy 418, 423. Jeffrey Carr, 'The misunderstood acronym: Why cyber weapons aren't WMD', (2013) 69 *Bulletin of the Atomic Scientists* 32, 34.

6 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) ('*Tallinn Manual 2.*0') 452.

7 Ibid.

8 Ibid.

FIGURE 1. REPRESENTATION OF THE RELATIONSHIP BETWEEN A CYBER SYSTEM, A SOFTWARE AND A CYBER WEAPON.



B. Weapons Review

Prohibitions and limitations on weapons are woven deeply into the fabric of IHL[9] and the principles and rules of IHL that regulate weapons are layered.[10] At the broadest level, some general principles and rules apply to all weapons under IHL.[11] Some weapons cannot be directed at a military objective or combatants and would be prohibited because they are inherently indiscriminate. The German V1 rockets used in World War II and the Scud missiles launched by Iraq during the First Gulf War of 1990-91 are examples of such weapons.[12] Beyond the general rules and principles, some treaties regulate or ban specific weapons or classes of weapons such as cluster munitions, landmines, chemical and biological weapons, incendiary weapons and blinding lasers. Finally, Article 36 of API requires State parties to do as follows:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[13]

9 Gary D. Solis, *The law of armed conflict: international humanitarian law in war* (2nd edn, CUP 2017) 5.
10 Robert Kolb and Richard Hyde, *An introduction to the international law of armed conflicts* (Hart Publishing, 2008) 153.
11 Ibid.
12 UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (Ministry of Defence, United Kingdom, 2004) 104.
13 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I), 8 June 1977.

This Article is also reflected in the *Tallinn Manual 2.0* as Rule 110 lit. (b). The IGE was divided on the question of whether Article 36 reflected customary international law or whether it is only applicable to States that have ratified API.[14] Moreover, Rule 110 is not completely exhausted by Article 36 of API, but also contains lit. (a). This rule sets out a customary obligation to ensure that applies to all States and requires them to ensure that the cyber means of warfare that they acquire or use comply with the rule of the law of armed conflict. In our opinion, some issues arise.

First, the nature of a legal review in lit. (a) is unsettled.[15] It remains questionable whether mere advice of a legal advisor on deployment and use satisfies this requirement. The IGE considered it sufficient,[16] taking a practical perspective, as the legal advisor might be the only available option.[17] Regarding lit. (b), there is an obligation to conduct a formal legal review[18] but it is not specified how the review mechanism should be established.[19] Countries such as the United States, the United Kingdom, Belgium, the Netherlands, Norway, Sweden, Australia, France or Germany already have established procedures of legal review for new weapons,[20] but there is no duty to disclose these mechanisms.[21]

Second, the issue of whether a State is party to an armed conflict is not the decisive factor for legal review.[22] Thus, States should carry out a legal review in advance. In this paper, we discuss whether we could imply the same for situations that are below the threshold of armed conflict. The deployment of specific software might trigger armed conflict, and the legal classification of conflict might only be specified after a lapse of time, based on facts of the conflict and further investigation. We therefore believe that software review in broader terms reflects the *ratio* of the existing legal framework.

3. BACKGROUND FOR SCENARIOS

For the purpose of further discussion, we present the following scenario involving the hypothetical escalation of conflict between two fictional States. Berylia and Crimsonia

14 *Tallinn Manual 2.0*, supra n. 6, 465. Compare Natalia Jevglevskaja, 'Weapons Review Obligation under Customary International Law', (2018) 94 *INT'L L. STUD* 186.
15 International Cyber Law: Cyber Law Toolkit. Scenario 10: 'Cyber Weapons Review', <https://cyberlaw.ccdcoe.org/wiki/Scenario_10:_Cyber_weapons_review> [accessed 17 December 2019].
16 *Tallinn Manual 2.0*, supra n. 6, 465.
17 William H. Boothby, *Weapons and the Law of Armed Conflict* (2nd edn, OUP 2016), 341.
18 Compare 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, Commentary 1987, par. 1970.
19 A Guide to the Legal Review of New Weapons, Means and Methods of Warfare, 20, <https://e-brief.icrc.org/wp-content/uploads/2016/09/12-A-Guide-to-the-Legal-Review-of-New-Weapons.pdf> [accessed 17 December 2019].
20 William H. Boothby, supra n. 17, 343.
21 Supra n. 18.
22 Supra n. 15.

are neighbouring countries.[23] For the purpose of an applicable international legal framework, Berylia is a signatory to the European Convention on Human Rights (ECHR) and API.

One of the Berylian regions directly neighbouring Crimsonia is historically disputed. Citizens of Berylia living in this region align themselves with the nationality that is dominant in Crimsonia. These citizens organise themselves into a political organisation, Crimson Home. The ultimate goal of Crimson Home is cessation from Berylia and incorporation into Crimsonia. Crimson Home intends to reach this goal through a political referendum.

For various reasons, including heightened geopolitical and regional ambitions, both States are prone to escalation of conflict through various triggering events of a cyber and non-cyber nature. These will be described below.

Before the conflict, Berylia had developed cyber capabilities to be able to collect, disrupt and potentially destroy data which adversaries rely upon. For this purpose, the Berylian government procured and developed cyber capabilities allowing the delivery of a harmful payload to target devices. Operators from Berylian law enforcement and armed forces are able to target specific networks or a specific range of IP addresses. Malware can be used to infect targeted devices and obtain sufficient rights to allow the remote delivery of a harmful payload to different components of an operating system. This payload includes modules allowing surveillance of communication, tracking of movement, issuance of counterfeit messages or erasure of data stored on the device. We will refer to this cyber system as Berylian Malware (BERM).

4. STATE VS. CITIZENS

1) Scenario

The first part of our scenario observes a deteriorating relationship between Berylia and Crimsonia. Crimson Home, actively seeking to secede from Berylia, is heavily financed from Crimsonia. The Crimsonian government, despite numerous allegations, has never admitted to supporting Crimson Home. However, finances pouring into Crimson Home originate, according to Berylian intelligence, from Crimsonian companies identified as shell companies used by the Crimsonian government.

After the Berylian government refuses to hold a referendum in conjunction with national elections, Crimson Home heightens its activity. Targeted ads sponsored by Crimson Home aim to incite tension between citizens living in the disputed region and the central Berylian government. This eventually leads to a series of rallies and

23 We follow the naming convention of fictional States used in Locked Shields exercises. However, this in no way implies any endorsement of our paper from any of the Locked Shields organisers.

protests. Social unrest results in small-scale riots, localised violence and spontaneous attacks on election officials and polls. No fatalities are reported, and a number of injured participants is limited to a minimum. Law enforcement agencies use tear gas to disperse the most stubborn protesters. This is directly followed by a series of arrests of people either directly participating in riots or suspected of organising and inciting them. Crimson Home is targeted by BERM. Payload effects include the surveillance of communications and tracking the movement of high-profile members of the organization.

The situation escalates when Crimson Home members organise bombings in the disputed region. These attacks are aimed mainly at buildings representing the central government, the legislature and the courts. The death toll quickly rises into the hundreds. This surge of violence is unprecedented and surprising to the Berylian government. Berylia responds by requiring Crimsonia to cease financing Crimson Home. At the same time, the Berylian government launches large scale operations involving law enforcement agencies as well as a limited deployment of Berylian armed forces in the disputed region. Tension in the region continues to rise. Crimson Home is further targeted by BERM. Payloads still conduct surveillance of communication and tracking of movement. After the bombings, the scale of BERM deployment is increased, and all known members of Crimson Home are targeted.

2) Legal Qualification

Understandably, any State must be aware of its human rights obligations stemming from international treaties. Berylia is obliged to secure rights and freedoms stemming from the ECHR. Nonetheless, Article 15 of ECHR[24] allows derogation from such an obligation. To achieve this, Berylia needs to determine whether a series of rallies, protests and riots is 'an exceptional situation of crisis or emergency, which affects the whole population and constitutes a threat to the organised life of the community of which the State is composed'.[25]

The fact that these events take place only in the disputed region is not an obstacle because 'a crisis which concerns only a particular region of the State can amount

24 Article 15 - Derogation in time of emergency
'1. In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under [the] Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.
2. No derogation from Article 2, except in respect of deaths resulting from lawful acts of war, or from Articles 3, 4 (§ 1) and 7 shall be made under this provision.
3. Any High Contracting Party availing itself of this right of derogation shall keep the Secretary General of the Council of Europe fully informed of the measures which it has taken and the reasons therefore. It shall also inform the Secretary General of the Council of Europe when such measures have ceased to operate and the provisions of the Convention are again being fully executed'.

25 European Court of Human Rights, *Lawless v. Ireland (No. 3)*, application no. 332/57, 1 July 1961, para. 28.

to a public emergency threatening ”the life of the nation”’.[26] The determination of the situation as a state of emergency is left to the State as a matter of margin of appreciation.[27] A State is not allowed to go beyond what is strictly required by the exigencies of the situation. Whether surveillance of communication and tracking of movement of high-profile members of an organisation complies with this requirement may be assessed against a set of factors based on judicial decisions of the European Court of Human Rights.[28] Assessment of the deployment of BERM when the situation escalates might be clearer if Berylia determines such acts as terrorism, as terrorism meets the standard of a public emergency.[29]

There are also other requirements, but their in-depth analysis is not relevant to this scenario. Therefore, prior to deployment of BERM, Berylia should ensure that its actual deployment will not violate the human rights of its citizens. This could be done by conducting a legal review of BERM against relevant legal obligations and possible derogations in a state of emergency. It is worth noting that clauses similar to Article 15 of ECHR exist within the International Covenant on Civil and Political Rights (Article 4) and the American Charter on Human Rights (Article 17).

5. STATE VS. STATE

A. Sovereignty

1) Scenario

Our scenario follows further escalation. Despite Berylia’s freezing bank accounts of the Crimson Home and its high-profile members as a part of ongoing counter-terrorism operation, Berylian intelligence confirms that Crimsonia has not stopped financing Crimson Home. Financing is now provided by couriers crossing the border from Crimsonia with large sums of cash. Berylian intelligence reports a strong suspicion that weapons are also being transported to Berylia as the Crimsonian government strengthens its support for Crimson Home. BERM is deployed to target any device that connects to specific cell towers located near the border. Payload activities include the surveillance of communication and of movement. However, selected individuals are targeted by harmful payloads allowing suppression of outgoing communication from their devices.

26 European Court of Human Rights, *Ireland v. the United Kingdom*, application no. 5310/71, 18 January 1978, para. 205.

27 European Court of Human Rights. Guide on Article 15 of the Convention. Derogation in time of emergency, para. 11.
< https://www.echr.coe.int/Documents/Guide_Art_15_ENG.pdf> [accessed 17 December 2019].

28 Supra n. 27, para. 21.

29 Supra n. 27, para. 12.

2) Legal qualification

Interstate relations come into consideration at this point. With couriers crossing borders with cash and potentially with weapons, Berylia might decide to consider this situation as a violation of its sovereignty. It seems appropriate to refer to the well-known *Island of Palmas* arbitral award where a definition of sovereignty was proposed,[30] the basic components of which were further developed in Article 2(4) of the UN Charter with key components of territorial integrity and political independence. Berylia might also consider whether to perceive sovereignty as a rule or as a principle. This is still a matter of debate, not only in academia,[31] but also in state practice.[32] It is important to note that Berylia needs to attribute the conduct of couriers to the Crimsonian authorities, as only States can violate sovereignty. The first act of violation of sovereignty deals with the territorial aspect. When a person physically crosses the borders with money and weapons, the involvement of state authorities is more likely than when done virtually by sending money. Berylia might also focus on alleged Crimsonian interference with Berylian governmental functions.

Even though these events are non-cyber in nature, they further fuel the escalation process. If Berylian claims that Crimsonia has violated its sovereignty prove correct, interstate tension will be escalated, and the legal background of this fictional conflict will change. In response, Crimsonia might claim that the deployment of BERM in the disputed region violates Crimsonian sovereignty. As BERM targets any device connecting to specific cell towers near the border, it is possible that the devices of Crimsonian citizens will also be affected. Therefore, it is important to examine BERM capabilities and possible targeting issues before deployment. In our scenario, Berylia should conduct a software review regarding the conditions which Crimsonia may take into consideration when labelling the deployment of BERM as a violation of sovereignty. Violation of sovereignty by cyber means remains an unsettled issue, and the IGE presented three levels which might be helpful to determine whether a violation of territorial sovereignty has occurred. These include considerations as to whether BERM is capable of causing physical damage, loss of functionality or infringement upon territorial integrity falling below the threshold of the loss of functionality.[33] It is also important whether the deployment of BERM leads to interference with the inherently governmental functions of Crimsonia.[34]

30 Island of Palmas Case (Netherland, USA), 4 April 1928, 838.

31 Michael N. Schmitt and Liis Vihul, 'Respect for Sovereignty in Cyberspace', (2017) 95 Texas Law Review 1639; Gary P. Corn and Robert Taylor. 'Sovereignty in the Age of Cyber', (2017) 111 AJIL Unbound 207.

32 Speech by the Attorney General Jeremy Wright at Chatham House delivered on 23 May 2018. < https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [accessed 17 December 2019].

33 *Tallinn Manual 2.0*, supra n. 6, 20.

34 *Tallinn Manual 2.0*, supra n. 6, 21.

B. Non-Intervention

1) Scenario

With the progression of the Berylian counter-terrorism operation, Crimson Home quickly depletes its human resources and its members are arrested or incapacitated as a direct result of actions by Berylian law enforcement and armed forces. The border, so far used for transportation of cash and weapons, is crossed by people willing to join Crimson Home. Berylian intelligence suggests that these volunteers are affiliated to Crimsonian paramilitary and military forces. However, direct and clear evidence is lacking. BERM is deployed to target devices connecting to specific cell towers located near the border. The payload still effects mainly surveillance of movement and surveillance of communication with intended recipients within Crimsonian territory.

2) Legal Qualification

The principle of non-intervention has very close ties to sovereignty. It is described as 'a corollary of the principle of the sovereign equality of States'.[35] Non-intervention mainly deals with the 'decision-making capacity of a State to formulate policies in relation to its internal and external affairs'.[36] The concept of internal and external affairs is flexible and linked to the notion of *domaine reservé*. The International Court of Justice (ICJ) sheds some light on the definition and has held that States may decide freely on matters such as 'choice of a political, economic, social and cultural system, and the formulation of foreign policy'.[37] That being said, not every coercion trying to violate this freedom of choice violates international law. Only coercive acts reaching a sufficient level of magnitude and intending a target State to change its policy are legally relevant.[38] However, this threshold is fluid and context-dependant.

Berylia might assess whether dozens of people crossing the border and willing to fight for Crimson Home constitute a violation of the principle of non-intervention. Individuals are not legally capable of violating the non-intervention principle. Therefore, Berylia should probably resort to a political attribution and make its suspicion of affiliation of volunteers to Crimsonian forces public. Berylia should also take into consideration the context and intent. Crimson Home sought to secede the region through a referendum and when denied, it turned to violence. *Ergo*, it is pushing for a change of Berylian policy with regard to the disputed region. If the personnel joining Crimson Home intend to force Berylia to change its position towards the region, it might suffice to establish an unlawful intervention.

35 ICJ, Case Concerning Military and Paramilitary Activities in and Against Nicaragua ('*Nicaragua v. United States of America*'), Judgment of 27 June 1986, para. 202.

36 Russell Buchan. 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 212, 223.

37 ICJ, *Nicaragua v. United States of America*, supra n. 35, para. 205.

38 Buchan, supra n. 36, 223-224.

Under international law, Berylia is entitled to engage in countermeasures. As BERM is already deployed, it might serve the purpose besides the collection of data for intelligence, counter-intelligence and law enforcement purposes. It would be necessary to conduct a software review to ascertain whether the use of BERM might further escalate the conflict by exceeding what are permissible countermeasures.

C. Use of Force vs. Armed Attack

1) Scenario

While BERM was previously used mainly to gather intelligence, in response to the violation of its borders Berylia engages in remote destruction of data on devices carried by people crossing the border. This leads to loss of data of many innocent citizens from both Berylia and Crimsonia and large-scale damage to and destruction of property. According to Berylian intelligence, this extreme measure was only partially effective in response to Crimson Home and its affiliates. Crimsonia officially and publicly denounces the deployment of BERM and the harmful payloads distributed through the system. The Crimsonian government also announces that appropriate measures will be undertaken in response. This results in cyber attacks against Berylian dual-use and military infrastructure. Most of these attacks are DDoS and ransomware, but Berylian intelligence reports that they are serving as decoys for large-scale intelligence gathering and espionage. The communications of Berylian forces engaged in ongoing Berylian counter-terrorism operations within the disputed region are jammed from Crimsonian territory.

2) Legal Qualification

Remote destruction of data escalated the situation. We argue that the Berylian action and Crimsonian reaction pushed the whole conflict over the threshold of the use of force, making it inconsistent with purposes enshrined in Article 2(4) of the UN Charter. The IGE partially followed the *scale and effect*s approach laid out by the ICJ,[39] and used this approach for the qualification of the unlawful use of force.[40] To ease the qualification, the IGE also used a set of eight factors[41] that outline factual considerations on whether to consider a given cyber operation as an unlawful use of force. Despite these factors not being norms of international law, they do provide basic cues along which to structure the legal response.[42]

Before using BERM to deploy payload that might lead to a violation of the prohibition of the use of force, Berylia should have conducted a legal review to assess the possible legal consequences to determine, amongst other things, whether the operation may

39 ICJ, *Nicaragua v. United States of America*, supra n. 35, para. 195.
40 *Tallinn Manual 2.0*, supra n. 6, 331.
41 Factors include severity, immediacy, directness, invasiveness, measurability, military character, State involvement and presumptive legality. Compare *Tallinn Manual 2.0*, supra n. 6, 334-336.
42 As emphasised by the IGE 'they are merely factors that influence states making use of force assessments; they are not formal legal criteria'. *Tallinn Manual 2.0*, 333.

lead to violation of Article 2(4) of the UN Charter. Furthermore, Article 51 of the UN Charter which grants a victim state the option to respond with force comes into play. Even though the majority of States perceive the gap between the use of force and an armed attack and distinguish 'the most grave forms of the use of force (those constituting an armed attack) from other less grave forms',[43] other approaches also exist in the international community. As Harold Koh said at the Inter-Agency Legal Conference in 2012, 'the United States has for a long time taken the position that the inherent right of self-defence potentially applies against any illegal use of force'[44] and rejected the existence of any threshold. The other theory called the accumulation of events doctrine was originally introduced by Israel in the 1970s and reflected a situation of terrorist attacks. Israel advocated a position that even though:

> 'each specific act of terrorism, or needle prick, may not qualify as an armed attack that entitles the victim State to respond legitimately with armed force, the totality of the incidents may demonstrate a systematic campaign of minor terrorist activities that does rise to the intolerable level of armed attack.'[45]

D. Armed Conflict

1) Scenario

Berylian intelligence has obtained conclusive proof that volunteers crossing the border from Crimsonia are predominantly members of the Crimsonian armed forces and their activities are being organised by the Crimsonian government. The Berylian government publicly accuse Crimsonia of plans to occupy the disputed region by force. Berylia deploys heavy weaponry to the border region as a follow-up to the counter-terrorism operation against Crimson Home. As part of the preparation for potential conflict, BERM is taken over by the military to ensure coordination of intelligence gathering and targeted incapacitation of devices throughout the disputed region.

Newly-deployed Berylian forces engage volunteers from Crimsonia. As one of the Berylian units engages Crimson Home members and volunteers close to the border, the Crimsonian Air Force attacks the unit. As a follow-up, Crimsonia claims that the military build-up in the disputed region signals a planned invasion by Berylia. The Crimsonian government opts to move units across the border to set up defensive positions on a mountain ridge on Berylian territory. In response, Berylian units engage the Crimsonian Army to prevent it from crossing the border to Berylia.

43 ICJ, Nicaragua v. United States of America, supra n. 35, para. 191.
44 Hongju Koh, Harold. 'International Law in Cyberspace', (2010) *Faculty Scholarship Series* 4854, 7.
45 Norman Menachem Feder, 'Reading the U.N. Charter Connotatively: Toward a New Definition of Armed Attack', (1987) 19 *N.Y.U. J. Int'l L. & Pol*. 395, 415.

2) Legal Qualification

We deem that the last round of escalation leads Berylia and Crimsonia into a state of armed conflict. As a result, the norms of IHL are triggered. Berylia is, as a signatory to the API, obliged to conduct a weapons review under Article 36 of API.

According to the IGE, all States, whether they have ratified API or not, are required to ensure that the means of warfare they acquire or use comply with the rules and principles of IHL. This obligation is derived from a general duty of compliance with IHL.[46] There are at least two points to highlight the weapons review process. First, IHL does not mandate States to establish a general practice of using a weapon before it is to be considered legal.[47] Second, the Commentary to API sheds light on the intent behind the weapons review. It requires States to determine whether the employment of a weapon for its expected use could be prohibited under IHL.[48]

6. DISCUSSION

Although the term 'weapons review' is frequently tossed around, there are different approaches not only between individual States, but also within States themselves. We can take the United States as an example. The United States did not ratify API and its views on reviewing the legality of weapons can be found in the *DoD Law of War Manual* from June 2015 (*the Manual*).[49] It is the position of the DoD to require a legal review for the intended acquisition or procurement of weapons or weapons systems.[50] Such a review should address three questions to determine whether the weapon's acquisition is prohibited with regard to U.S. DoD obligations: (1) whether the weapon's intended use will cause superfluous injury; (2) whether the weapon is inherently indiscriminate; and (3) whether the weapon falls within a type that has been specifically prohibited.[51] U.S. DoD approaches these legal reviews in two stages. The first is an evaluation of the weapon to determine whether its use would be illegal *per se*. The second is to determine whether its use in a particular operation could be illegal.[52] The *Manual* also addresses the legal review of weapons employing cyber capabilities. It notes that not all cyber capabilities constitute a weapon and it is up to individual branches (i.e. Army, Navy, Air Force) of the US armed forces to determine which cyber capabilities require legal review. The *Manual* highlights the most obvious

46 *Tallinn Manual 2.0*, supra n. 6, 464-465. The IGE commented that this duty of compliance is reflected in Article 1 of the 1907 Hague Convention IV and Common Article 1 of the 1949 Geneva Conventions.

47 Office of General Counsel, Department of Defence, *Department of Defence Law of War Manual 338* (2015, updated 2016).

48 Louise Doswald-Beck and Jean-Marie Henckaerts. Customary International Humanitarian Law 237 (2005). The basis for this principle, which reflects customary international law, is Article 23(e) of the Hague Regulations and Article 35(2) of API.

49 *DoD Law of War Manual*, supra n. 46, 337.

50 Ibid.

51 Ibid., 338-9.

52 Ibid., 1025.

IHL related concern, which is the potentially indiscriminate effect of a cyber weapon. It notes that a destructive computer virus designed and intended to spread and destroy uncontrollably within the civilian internet systems and networks would be prohibited under IHL as an inherently indiscriminate weapon.[53]

The term 'weapon' is used in different contexts and often without the normative meaning given to it by international law. The same could be said of the term 'weapons review', as it immediately brings out requirements according to Article 36 of API.

That being said, it is undeniable that the use of software for security purposes has consequences in terms of international law both in State-to-State and State-to-individual relationships. Additionally, individual cyber systems can be used to deliver different payloads, and it is hard to pinpoint the exact moment at which the payload becomes a weapon. A broader understanding of software review concerning international law obligations is sensible. We argue that this sort of review entails practical necessity. The development of new software might be quite costly and the guide to the legal review of new weapons states 'conducting legal reviews at the earliest possible stage is to avoid costly advances in the procurement process (which can take several years)'.[54] This applies even outside armed conflict and the weapons review prescribed in Article 36 of API.

The violation of legal obligations, as our scenarios illustrate, can happen on many different levels in conflict. Article 36 of API prescribes review to prevent the violation of IHL norms. We argue that a system of broader software review would bring (1) more understanding of legal consequences in general, and (2) better framing of policy responses in terms of escalation and de-escalation of potential conflicts.

7. CONCLUSION

In formulating our research question of what legal requirements need to be considered when deploying cyber weapon in situations below the threshold of armed conflict, our broader intent was to evaluate whether the requirement of legal review of cyber weapons or capabilities exists outside IHL. We used a fictional scenario of an escalating conflict, presented basic facts and legal qualification of different events.

The conclusion is, there are plenty of legal requirements to be considered when deploying cyber means. These range from human rights obligations and their possible derogation in case of internal emergency all the way to IHL in armed conflict. Rather unsurprisingly, we conclude that there is no obligation to conduct a review outside Article 36 of API. However, in terms of practical necessity, it is worth considering

53 Ibid., 1025-6.
54 *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare*, supra n. 19, 20.

a broader software review. This would allow more respect to international law obligations by prior evaluation if any software, whether considered a cyber weapon or not, violates the international law obligations of a State.

Cyberspace has brought to light many definitional issues that are still unresolved. A broader approach to software review will allow us to understand the use of software in context and eventually bypass the normative outcomes of labelling something a cyber weapon. We conclude there is no obligation to conduct weapons review outside Article 36 of API. That being said, we believe there are policy benefits in conducting broader software assessments with regard to legal obligations.