CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Data as a Weapon: Refined Cyber Capabilities Under Weapon Reviews and International Human Rights Law

Samuele De Tomas Colatin
NATO CCDCOE, Legal researcher

Ann Väljataga
NATO CCDCOE, Legal researcher

Tallinn 2020

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 25 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the Tallinn Manual 2.0, the most comprehensive guide on how International Law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise Locked Shields. Every spring the Centre hosts in Tallinn the International Conference on Cyber Conflict, CyCon, a unique event joining key experts and decision-makers of the global cyber defence community. From January 2018 CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations - to this date Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom, and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Table of Contents

Introduction

In 2012 it was estimated that around 120 states had introduced some form of cyber weapon development programme[1] and there is no reason to expect the number to have dropped since then. However, exactly what constitutes a cyber weapon is still a matter of dispute, which is why the term 'capability' is often preferred. We can nevertheless be sure that when a piece of computer code is classified as a weapon, means or method of warfare under international law, it will be subject to legal review according to Protocol I Additional to the 1949 Geneva Conventions. While there is considerable *opinio juris* and state practice to declare weapons reviews a customary international law obligation and the US, for instance, has not ratified AP II, to date the obligation is held to be rooted in treaty law. Article 36 requires states to conduct a legal review of all new weapons, means and methods of warfare to ensure that their deployment would comply with international law:

> 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.[2]

Cyber capability development is a complex and time-consuming procedure, further complicated by the fact that sophisticated cyber weaponry is tailored to a specific target and data exploit software forms an integral part of it. Getting to know the target, its functioning and vulnerabilities takes up a large share of the development and deployment procedure, whereas the actual attack may consist of the mere act of pressing a button. This kind of systemic protracted covert information gathering typically belongs to the arsenal of intelligence services, rather than that of military cyber security officers or the arms industry.

In 2014 former NSA and CIA Director Michael Hayden stated that he could think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones), and that the secretive heritage of intelligence practices was hampering the progress towards effective regulatory policies.[3] Senior Vice President at the Centre for Strategic and International Studies James Lewis has noted that since the network penetration and control necessary for espionage could be used to disrupt critical services, the line between espionage and attack in cyberspace is very thin and an opponent who can gain controlling access to a network can also disrupt and perhaps destroy it.[4]

The espionage component of cyber capabilities also implies that the attacker possibly engages actively with the target system years before the actual attack, and so first access and data exploits often takes place during peacetime. The merging of espionage and the deployment of a cyber capability implies that while one is accessing, copying and analysing the necessary data, one might already be using the capability or at the very least be building it, even though the planned final effects of the operation are yet to emerge. Taking this as a point of departure, this paper will analyse Article 36 weapons reviews while considering the uniqueness of the atypical development and deployment of cyber capabilities. In parallel, it examines how the same procedures of development and deployment would be regulated under peacetime international human rights law (IHRL). Ultimately, the research will shed light on the

---

[1] Infosec, The Rise of Cyber Weapons and Relative Impact on Cyberspace, https://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace/, 5 October 2012
[2] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1125 U.N.T.S. 3 (June 8, 1977).
[3] Lin, Herbert, and Amy Zegart, eds. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Brookings Institution Press, 2019.
[4] Lewis, James A., 'In defense of Stuxnet' *Military and Strategic Affairs* 4, no. 3 (2012): 65-76, 66.

nature of the legal regime best suited for regulating sophisticated cyber capabilities, taking into account different stages of their development.

Applicability of Article 36

Article 36 applies to certain cyber capabilities. This assertion underpins this paper and follows from the acknowledgement that these cyber capabilities are a) weapons b) means of warfare or c) methods of warfare. The Geneva Conventions and their protocols offer no guidance to define these categories. A comparative analysis by Schmitt and Biller concludes that state as well as unofficial definitions of the term 'weapon' tend to refer as the determinative factor to the potential to cause direct damage to objects or individuals in combination with respective intent.[5] The *Tallinn Manual* defines cyber weapons as:

> 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, that is, which result in the consequences required for qualification of a cyber operation as an attack.[6]

A 'cyber means of warfare' encompasses 'cyber weapons and their associated cyber systems', including 'any cyber device, material, instrument, mechanism, equipment, or software used, designed, or intended to be used to conduct a cyber attack'. Methods of cyber warfare are defined as 'the cyber tactics, techniques, and procedures by which hostilities are conducted' and refer to 'how cyber operations are mounted, as distinct from the means used to mount them'. As there is no source of customary or treaty law which offers a legal definition for any of the three terms, in practice the meaning of each of these is dependent on context-specific interpretations by states.

Biller and Schmitt argue that since computer code cannot directly inflict damage, it fails to qualify as a weapon or means of warfare.[7][8] A different approach would infer that a cyber capability could be granted the status of a weapon or means of warfare by virtue of the second-order effects it causes. For instance, the recent Danish Joint Doctrine for Military Cyberspace Operations, in which a cyber weapon is defined as computer code applied to create the desired effect on the target, states that the effects can be both physical and virtual.[9] Likewise, Boothby defines a cyber weapon as an 'object, device, munition, or equipment used to apply an offensive capability'.

While ruling out classifying a piece of computer code as a weapon or means, Biller and Schmitt and Biller see no reason for not fitting it under the notion of 'methods of warfare.' In software, they see a digital sequence of instructions which describe *how* a cyber operation will be executed, from the very moment of access until the realisation of the final effects, thereby admitting that the obligation to conduct legal reviews continues to apply. Therefore, whether or not we set the capacity to directly cause damage or destruction as an essential feature of a cyber weapon has no impact on the applicability of Article 36, and hence remains outside the scope of this article.

---

[5] Biller, Jeffrey T. and Schmitt, Michael N. 'Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare. Means, or Methods of Warfare' (June 19, 2019), 95
[6] Schmitt, Michael N. (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017), 452.
[7] Ibid.
[8] Biller, Schmitt, n 5, 92.
[9] Royal Danish Defense College, Joint Doctrine for Military Cyberspace Operations, (September 2019), 24.

Blurred lines between cyber espionage and cyber capabilities

The example of Stuxnet illustrates just how much the genesis of a complex cyber capability deviates from the standard life-cycle of a conventional weapon. Much ink has been spilt on the technical specifications, not to mention the political and legal impact, of Stuxnet; yet, almost a decade after its discovery, Stuxnet still serves as the epitome of a refined autonomous malware and has proven to be a true 'gift that keeps on giving' for cyber researchers and strategists. While the odds are that the technological realities have moved on, in terms of the quality and abundance of documented information available, Stuxnet is yet to meet an equal. It is not rare to find references to Stuxnet as a 'cyber espionage tool' in the media and even in peer-reviewed journals and specialised magazines or blogs[10] and, while imperfect, this is not a complete misnomer as it is equally imperfect to see in Stuxnet only a cyber weapon.

The essence of Stuxnet that made the manipulation of Natanz uranium centrifuges possible was a set of sophisticated cyber espionage tools. After entering the target system, Stuxnet would record its operations and gather and store data. It was designed to perform a full array of data exploit operations that would later enable to gain control over programmable logic controllers in the nuclear plant.[11] First, the creators wrote a so-called beacon program which was designed to map out the workings of the nuclear enrichment centre at Natanz. Once it had entered its target system, the program collected information on how the plant's computers were configured and transmitted that data back to the owning intelligence agencies. The collected data was then put to use and a new program was introduced to the plant's computer controllers which successfully took over the operation of some centrifuges and manipulated them into malfunctioning through the regular insertion of incorrect data. Therefore, while the damage was done by attacking the integrity of the information on which the control systems were reliant, the scenery was set through data exploitation.[12] As we can see, the exact moment, where espionage ended and a cyber capability was deployed is difficult to pinpoint.

The espionage-focused cousin of Stuxnet, Duqu, was discovered by Hungarian security researchers in 2011 in the aftermath of the unveiling of its more aggressively disruptive counterpart. Duqu is a remote access Trojan that shares its source code with Stuxnet and is believed to have been created by the same authors. Duqu contained three main groups of malware: a standalone keylogger, a module designed to store and transmit configuration data and an encryption module.[13] Therefore, while lacking a disruptive capability, it aimed to gather intelligence data that could later enable cyber weapons such as Stuxnet to achieve their design objective.

While real-life cyber capabilities remain behind a veil of secrecy, the *Tallinn Manual 2.0* contains a fictional example of an integrated espionage software whose legality should be determined in reference to the whole operation. The majority of *Tallinn Manual* experts agreed that, although acts of cyber

---

[10] See eg. Gibbs, Mark, 'Why Stuxnet is a really bad weapon' *NetworkWorld*, (22 June 2012) https://www.networkworld.com/article/2189571/why-stuxnet-is-a-really-bad-weapon.html; McMillan, Robert 'Siemens confirms German customer hit by Stuxnet espionage worm' *InfoWorld* (21 July 2010) https://www.infoworld.com/article/2625529/siemens-confirms-german-customer-hit-by-stuxnet-espionage-worm.html.

[11] Langner, Ralph, 'Stuxnet: Dissecting a cyberwarfare weapon' (2011) 9 *IEEE Security & Privacy Magazine* 49

[12] Ibid.

[13] Bencsáth, B., Pék, G., Buttyán, L., & Felegyhazi, M. 'The cousins of Stuxnet: Duqu, Flame, and Gauss' (2012) *Future Internet*, *4*(4), 975.

espionage may not be unlawful in themselves, they can nevertheless constitute an integral and indispensable component of an operation that violates international law,[14] thereby hinting that cyber capabilities evade compartmentalisation. The *Manual* drafts a scenario of a state that executes a single plan in which it employs cyber espionage to acquire the credentials necessary to access the industrial control system of a nuclear power plant of another state, with the intent of threatening to conduct cyber operations against the system in a manner that will cause significant damage or death unless the former ends particular military operations abroad. The majority of experts took the view that once the threat had been communicated, the action in its entirety, including the integrated cyber espionage, constituted an unlawful threat of the use of force.[15] This once again emphasises that the legality of a cyber operation which is reliant upon cyber espionage should be assessed in its entirety.[16] This can only mean that the capabilities used for such integrated operations should also be so assessed.

In July 2011, the US Air Force updated Instruction 51-402, which marked a change in its definition of 'weapon' and foresaw a legal review of cyber capabilities intended for use in cyberspace operations. The Instruction requires that cyber capabilities, like weapons 'being developed, bought, built, modified or otherwise being acquired by the Air Force,' 'be reviewed for legality under the Law of Armed Conflict, domestic law and international law prior to their possible acquisition for use in a conflict or other military operation'.[17] Blount notes that, although they receive the same legal review, cyber capabilities are not termed as weapons. Weapons, for the Instruction's purposes, are 'devices designed to kill, injure, disable or temporarily incapacitate people or destroy, damage or temporarily incapacitate property or material'. Air Force Instructions recognise that, in most instances, a cyber weapon is not a device but a software package or technique. Cyber capabilities, under the Instructions, constitute 'any device[s] or software payload[s] intended to disrupt, deny, degrade, negate, in air or destroy adversarial computer systems, data, activities or capabilities'.

The drafters of the updated Instructions seem to acknowledge the degree to which espionage forms the essential groundwork of any cyber capability, and seem keen on remaining true to the unregulated grey-area nature of espionage. They state that devices and software that are 'solely intended to provide access to an adversarial computer system for data exploitation do not need legal review'.[18] In practice, this distinction would only prove adequate when applied to programs of a very narrow functional use and not to more comprehensive and sophisticated software packages. A more efficient and complex program that breaks into a system, exploits the data, analyses it, and designs or possibly even executes operations based on the foregoing analyses, would fall outside the exception. Therefore, a program that has data exploitation as one of its core functions amongst others is still likely to go under legal review in its entirety. Air Force Instruction 51-402 stands out since it is the only official document that, albeit tacitly, recognises the degree to which cyber capabilities are bound to cyber espionage and deliberately avoids subjecting tools of data exploitation to weapons review.

Rid and MacBurney understand a cyber weapon as 'a tool used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things'.[19] According to them, a piece of malware that is intended to commit cyber espionage against another State is not considered a cyber weapon, whereas they note that high-potential cyber-weapons may require

---

[14] Schmitt, n 5, 171.
[15] Ibid.
[16] Blount, P. J. 'The preoperational legal review of cyber capabilities: Ensuring the legality of cyber weapons' (2012) *N. Ky. L. Rev.*, *39*, 211.
[17] *See* United States Air Force, Legal Reviews of Weapons and Cyber Capabilities, A.F. INSTRUCTION 51-402 (July 27, 2011), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-053.pdf.
[18] Ibid.
[19] Rid, Thomas, and Peter McBurney, 'Cyber-weapons' *the RUSI Journal* 157, no. 1 (2012): 6-13.

specific target intelligence that is programmed into the weapon system itself.[20] Representing a slightly different and more holistic point of view, Lewis compares cyber attacks to a weaponised form of signals intelligence that transforms the passive collection of signals intelligence into active disruption. Lewis notes that such conceptualisation would imply that to ban a cyber attack we would also need to ban espionage, therefore admitting that the espionage component cannot and should not be artificially separated from the whole concept of a cyber attack.[21]

The definition of a cyber weapon, method or means of warfare is conditional on what exactly is thought to constitute a cyber attack. According to the *Tallinn Manual* experts, a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. In the case of cyber weapons, physical injury or death is usually a second-order effect and not the direct intended outcome of the employment of the weapon.[22] The mere copying of resting or transit data could rarely, if ever, meet the definition of a cyber attack, and so software designed for this purpose would not be deemed a weapon. Wallace sees a catch in such a general statement and asks if this would exclude intelligence from the scope of application of weapons reviews, in cases where they are an indispensable precursor to the development and use of a cyber weapon to the point that the two are inextricably linked.[23]

While the question has often been tiptoed around, we find a rather straightforward answer from McClelland. He argues that, provided it is intended to be used in an attack, a system that is used to analyse target data and then provide a target solution or profile would reasonably fall within the meaning of 'means and methods of warfare'.[24] These statements gain a more practical and concrete dimension in the case of the cyber attack intended to disable Iran's maritime operations that was launched by the United States in June 2019. Often the attack has been described as a direct response to the destruction of a Global Hawk surveillance drone that took place on 20 June. In reality, the anatomy and timeline of the operation formed anything but a simple tit-for-tat reaction to one particular incident. 'We didn't just press a button,' Herbert Lin, senior cyber security scholar at Stanford, explained. 'We'd done lots of work in advance to figure out what targets to hit and to maintain access to them. That happened months and years ago.'[25] When viewed in light of the arguments made by McClelland, the operations that operations preceded the cyber attacks against Iran would fall within the category of 'means and methods of warfare'.

The fading borders between cyber espionage and use of a cyber capability are widely recognised, whereas the conclusions drawn and solutions suggested vary enormously. If it is possible to highlight a single predominant line of thought, it would most probably be that wherever the border is drawn, it is likely to be artificial and to become obsolete in the course of technological development. Viewing these two holistically as parts of a single capability implies that the laws regulating weapons reviews and intelligence oversight should interact. Moreover, since cyber weapons are indeed often activated before entering the realm of *jus ad bellum* or *in bello*, the legal framework that provides better protection during peacetime should be given priority.

---

[20] Ibid.
[21] Lewis, n 4, 68.
[22] Schmitt, n 9, 417-418.
[23] Wallace, David, Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis (2018) Tallinn Paper no 11, 22.
[24] McClelland, Justin. 'The review of weapons in accordance with Article 36 of Additional Protocol I'. *International Review of the Red Cross* 85, no. 850 (2003), 405-406.
[25] Halpern, Sue, 'How cyber weapons are changing the landscape of modern warfare', *New Yorker* (18 July 2019).

Atypical life-cycle of a cyber capability – what and when should be reviewed?

In the previous section, it was argued that data exploits form an integral part of a cyber capability which is already activated when the target system is being accessed for intelligence gathering purposes. Although there is considerable support for this argument, due to the lack of publicly available technical studies, case law or official statements, another perspective also deserves some examination. Even in cases where the technical and strategic circumstances allow the perception of cyber espionage as separate from the weapon, it might still be subject to review obligations under Article 36. The obligation to review applies in the phases of study, development, acquisition or adoption of a weapon, method or means of warfare. Therefore, the issue is whether the built-in intelligence gathering might form an essential part of the study or development phase.

The ICRC guide to weapons reviews states as the aim of Article 36 to:

> prevent the use of weapons that would violate international law in all circumstances and to impose restrictions on the use of weapons that would violate international law in some circumstances, by determining their lawfulness before they are developed, acquired or otherwise applied or otherwise incorporated into a State's arsenal.[26]

The commentary restricts the scope of the weapons review obligation to 'the normal use of the weapon, means or method of warfare as anticipated at the time of the evaluation'.[27] Therefore, the commentary views the use of the capability as the object of review. Due to their atypical life-cycles, cyber capabilities tend not to make a linear transition from preparation to use and this might justify a different timing and emphasis in the review procedure. The current section takes the position that, even when it proves technically possible to treat integrated cyber espionage as distinct from the employment of the weapon, against the current and near-future technological backdrop it might nevertheless make sense to subject it to legal review as an integral part of the development procedure.

The plain wording of Article 36 suggests that the obligation for states starts at a very early stage of the acquisition process. Article 36 lists the 'study" of a weapon and this might imply that a legal assessment should at least be considered even before entering the development process of a new weapon or technology. Supporting this argument, Boothby states that even technology that would be potentially capable of weaponisation needs attention.[28] He argues that whenever a weapon, means or method is being studied, the weapons review duty applies, and adds that it will be a matter for national judgement when general technology research becomes the study of a weapon.[29] It has been suggested that this happens when particular kinds of weaponisation are being first discussed or evaluated.[30] Therefore, advice of a legal nature is required from the very moment a weapon or a method of warfare is being actively evaluated.

Boothby does not clarify which activities are encompassed by the notion of study of a weapon, but it can be assumed that it refers to scientific research related to the designed weapon. If that research entails gathering information about the target system, then intrusions for cyber espionage would fall within the

---

[26] ICRC, 'A Guide to the Legal Review of New Weapons, Means and Method of Warfare – Measures to implement Article 36 of Additional Protocol I of 1977', (January 2006), 4.
[27] Ibid.
[28] Boothby, William H., 'How Will Weapons Reviews Address the Challenges Posed by New Technologies' (2013) 52 *Mil L & L War Rev* 37, 39
[29] Boothby, William H. *Weapons and the Law of Armed Conflict*. (Oxford University Press, 2016), 353
[30] Boothby (2013), n 37.

concept. Development, according to Boothby, involves the application of materials, equipment and other elements to form a weapon and includes the improvement, refinement and probably the testing of prototype weapons to achieve optimal performance. If the data which is collected through cyber espionage is connected and applied in a way that directly supports the planned effects of the weapon, then ongoing data collection and analysis constitute the base of the development phase

While endeavouring to define the concept development of a weapon, Casey-Maslen and Vestner conclude that, although there is no agreed legal definition, a glance into everyday parlance and disarmament treaties might help to clarify the matter. 'Developing' something usually refers to the process of creating or producing something, especially by deliberate effort over time. Thus, when applied to weapons, the ordinary meaning encompasses associated research and testing, including computer modelling, simulations and construction of a prototype.[31] In disarmament treaties, we find evidence that in some circumstances the development procedure itself becomes the object of regulation. The 1992 Chemical Weapons Convention conceptualises development as the preparation for the production of chemical weapons, as distinct from permitted research in the fields of medicine or pharmaceuticals, for example.[32] The authors note that the ambit of the 2008 Convention on Cluster Munitions is broader, covering the prohibition on direct and indirect development. Such a prohibition would outlaw the construction or procurement of parts and components with a view to their incorporation in the weapon, and also offshore licensing agreements.[33] Therefore, although viewing the development process itself as subject to review and regulation under international weapons law is not entirely unprecedented, it has never before proved as relevant as in the context of new technologies.

The phrasing of Article 36 indicates that the employment of the weapon is to be reviewed and not the development procedure itself. However, from a more teleological angle, this rarely serves the aims of Article 36 as applied to cyber capabilities, since they are usually tested and developed in the field on the very target that they are meant to exploit and their effects are of a more gradual and cumulative nature[34] The latter calls for a review procedure that is initiated as early as possible and goes beyond the concept of 'normal expected use'.

The International Committee for the Red Cross, in its 2019 *Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, highlighted that the unique characteristics of new technologies and the related processes of legal review require new standards of testing and validation.[35] When referring to autonomous weapons systems, the Report states that legal reviews of weapons, means and methods of warfare relying on these new technologies may need to be conducted at an earlier stage of the weapon life-cycle and at shorter intervals than for more traditional technologies, and may need to be repeated during development.[36] The primary trigger for the necessity for an updated

---

[31] Casey-Maslen, Stuart, and Tobias Vestner *A Guide to International Disarmament Law (*Routledge, 2019) 213.
[32] United Nations, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (and Protocols) (As Amended on 21 December 2001), 10 October 1980, 1342 UNTS 137, available at: https://www.refworld.org/docid/3ae6b3ac4.htm, cf Casey-Maslen and Vestner (n 30).
[33] United Nations, Treaty Series, vol. 2688, p. 39; depositary notification C.N.776.2008.TREATIES-2 of 10 Nov 2008, cf Casey-Maslen and Vestner (n 30).
[34] Even though Article 36 does not require States to analyse all possible foreseeable undesired effects or misuses of a weapon, the ICRC is recognizing that, as weapon system become more complex and are given more freedom of action in their tasks, it is impossible to simulate a testing environment which would reflect a dynamic real world scenario and would take into account unpredictability in the functioning of the considered system. Thus, even predicting foreseeable undesired effects becomes challenging. ICRC, 'International humanitarian law and the challenges of contemporary armed conflicts', (2019), 29, available at: https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf.
[35] Ibid, 29.
[36] Ibid, 29.

review procedure is the degree of unforeseeability that these technologies yield. Traditional review methods only focus on the normal use of the weapon as anticipated at the time of the evaluation, and are therefore likely to fall short on precision and substance when faced with sophisticated cyber weapons with autonomous features. Potentially, the limited capacity to predict and review effects can be mitigated by meticulous legal review of the development procedures. Provided that the gathering and analysis of data forms an essential step in the development of any given cyber capability, it will not fall outside the scope of Article 36. This claim is based on the twofold premises of the requirement to conduct reviews at the earliest stages of the life-cycle and on the fact that fixing the gaze solely on potential use might prove myopic when dealing with advanced cyber technologies.

The idea that Article 36 manifests its obligations during the development of a weapon system is not novel. Referring once again to autonomous weapon systems, the ICRC maintains that to be able to respect the existing rules in the conduct of hostilities, a new cyber capability subject to review needs to implement certain limitations during the development and testing phase.[37] In fact, control exercised by the developer of the capability can take various forms within the life cycle of a weapon, including its programming.[38] It might be inferred that, to assess whether foreseeable effects will breach international law and the laws of armed conflict, the most suitable phase in which to include limitations and instructions within the novel cyber capabilities is the development and testing phase.

The emergence of autonomous weapons systems has led to a wider recognition of the need for clear and standardised review procedures.[39] The discussion over the application of Article 36 for autonomous weapons is currently conducted within the UN CCW CCE forum, the aims of which are prohibiting or restricting the use of certain conventional weapons and contributing to the process of disarmament. The UN Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems is seeking a legal framework in which to include certain autonomous capabilities and technologies still under development.[40][41] Even though the current CCW discussion is mainly concerned with lethal autonomous capabilities, the lethality feature makes up only a fraction of the problem and the deliberations around autonomy and foreseeability are easily applied to advanced cyber capabilities.

States are discussing how and when Article 36 obligations begin, and the interconnection with the legal review process which is apparently strictly related to the development phases. The Australian submission to the 2018 CCW GGE confirms that legal advisors review instruments and platforms which support the employment of a weapon, and new methods of warfare detailed in defence doctrine, instructions or documented procedures.[42] The Australian working paper considers the procurement process as the source of the Article 36 review, putting great importance on the various early stages

---

[37] ICRC, 'Views of the International Committee of the Red Cross (ICRC) on Autonomous Weapon System' (11 April 2016) UN Doc < https://www.unog.ch/80256EDD006B8954/(httpAssets)/B3834B2C62344053C1257F9400491826/$file/2016_LAWS+MX_CountryPaper_ICRC.pdf >

[38] Ibid, 3-4.

[39] UNIDIR finds that increasing autonomous features that are present in both physical systems and in cyber operations is creating a normative overlap between the two domains. *See*, UNIDIR Resources, 'The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations', https://unidir.org/publication/weaponization-increasingly-autonomous-technologies-autonomous-weapon-systems-and-cyber, UNIDIR, (16 November 2017), 5-8.

[40] Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, (13 December 2019) UN Doc CCW/MSP/2019/9 , Annex III.

[41] UN Chronicle, 'The Role of the United Nations in Addressing Emerging Technologies in the Area of Lethal Autonomous Weaons System' (December 2018) Vol. LV Nos. 3 & 4, 2018 <https://unchronicle.un.org/article/role-united-nations-addressing-emerging-technologies-area-lethal-autonomous-weapons-systems>.

[42] See, Australia, 'The Australian Article 36 Review Process' (30 August 2018) UN Doc CCW/GGE.2/2018/WP.6, para 9.

listed by the provision. Australia affirms that the whole review process is supporting the movement of weapons through the various phases of their capability life cycle, thus creating a strong bond between the first stages of the development process, the intended use of the capability and the scope of the obligation.[43] So far, the limited available state practice suggests that states favour reviewing new cyber military capabilities at an earlier stage of development, and at shorter intervals than for more traditional technologies. Interim Article 36 reviews will be conducted and repeated during the major 'decision-point' of the capability life cycle, eventually forming a final legal assessment.[44] Argentina recognises the gaps in the mechanism of revision of the new weapons means and method of warfare, suggesting that the stages of study, development, acquisition or adoption need detailed review.[45] The Netherlands and Switzerland, in their *Weapons Review Mechanism* CCW Working Paper,[46] maintain that the review obligation is met when the new capability is assessed as such, and also according to its intended use. This means that a cyber capability able to perform multiple functions which gains access to a foreign adversary's network through built-in intelligence cannot be seen just as a series of separate enabling features that would trigger subsequent effects, but rather as a unique package with embedded features that have to be implemented during the design and development process, therefore requiring legal assessment at an earlier stage. The first stages of the development of a cyber capability thus become relevant for addressing the built-in intelligence or data gathering processes which act as the *raison d'être* for producing the cyber capability.

From the previous analysis, mostly based on scarce publicly-available state practice and the 2006 ICRC guide of the legal review of new weapons, the need to consider the employment of a new capability is an inherent part of the early study process. This assumption will deliver a credible legal review in accordance with Article 36. There is no doubt that Article 36 applies to new cyber capabilities, but states are now discussing when and how the obligation starts, so that they can identify whether new standards of testing and validation are required. New cyber capabilities are blurring the lines between actual employment and the law of targeting, and *ad hoc* features designed within the cyber capability will also affect the way legal reviews are conducted.[47] A mere weapon law opinion is insufficient when reviews are conducted, since very specific planned circumstances of use have to be taken into account. Operational legal reviews conducted before the deployment or activation of certain cyber capabilities might prove insufficient for two reasons: first, that autonomous features embedded within the cyber capability trigger the desired effects when specific requirements are satisfied in a system which is characterised by a dynamic environment, making it very hard to predict even foreseeable undesired effects; and second, the very nature of the capability might already not be lawful in its design. A review that focuses strictly on the imaginable uses during a potential future armed conflict and overlooks the procedures of study and development might also go against the very purpose of Article 36 and prove both misleading and counterproductive.

---

[43] Australia defines the Capability Life Cycle as the process of introducing, sustaining, upgrading and replacing Defence capability. Ibid, para 12.
[44] Ibid, 3-4.
[45] Argentina, 'Strengthening of the Review Mechanism of a New Weapon, Means and Method of Warfare' (4 April 2018) UN Doc , CCW/GGE.1/2018/WP.2, 3 https://www.unog.ch/80256EDD006B8954/(httpAssets)/CBEC4BBE57288083C1258266002E980D/$file/CCW_GGE.1_2018_WP.2.En.pdf.
[46] The Netherlands and Switzerland, 'Weapons Review Mechanism' (7 November 2017) UN Doc CCW/GGE.1/2017/WP.5, 2.
[47] Boothby, Bill, 'How will weapons review address the challenges posed by new technologies?', (2013) 52 *Mil L & L War* Rev 37, 49-50.

International human rights standards as criteria for reviewing the legality of a cyber capability

There are two overarching reasons for turning to international human rights law (IHRL) when judging the legality of a weapon system. First, weapons, and especially cyber weapons, are often deployed outside the context of an armed conflict, either for law enforcement, for peacetime espionage purposes or for conducting under-the-threshold operations. Also, for reasons of precision and efficacy, cyber weapons have to be prepared during peacetime. If a weapon is to be deployed during armed conflict, the targets have to be identified and mapped long before a conflict has arisen. The information systems of the target have to be accessed, monitored and potentially manipulated or sabotaged during the initial phases of weapons development. However, these initial phases are not merely passive acts of observation,[48] but rather when the attacker interacts with the target system in real time. Anything that happens during these initial phases is within the scope of application of IHRL. Secondly, even in armed conflict fundamental human rights continue to apply and at times are given priority over IHL.[49] Overlooking IHRL when assessing the legality of cyber operations is counterintuitive since the lines between IHL and IHRL review standards are obfuscated in the cyber domain due to its fundamentally dual-use character.

Another reason for incorporating IHRL in the weapons review process is rather self-explanatory. Article 36 unambiguously lays down the obligation not only to determine whether the employment of a weapon would be prohibited by AP I, but also to ensure the compliance with 'any other rule of international law applicable to the High Contracting Party'. It is difficult to come up with a good reason why this should not include IHRL, yet we look in vain for a suitable historical comparison – cyber weaponry is unprecedentedly suitable for covert peacetime use and under-the-threshold operations. Therefore, provided that the espionage modes of the software cannot be separated from those directly causing the effects and they already engage with the target during peacetime, any IHRL rule applicable to cyber espionage acquires critical importance.

In Rule 32 of the *Tallinn Manual 2.0,* the term 'cyber espionage' is used to refer to any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather, or attempt to gather, information. The concept involves, but is not limited to, the use of cyber capabilities to closely observe, monitor, capture or exfiltrate electronically transmitted or stored communications, data or other information.[50]

Ziolkowski summarises the essence of cyber espionage as:

> copying of data that is publicly not available and which is in wireless transmission, saved or temporarily available on IT systems or computer networks located on the territory or area under the exclusive jurisdiction of another state by a state organ, agent, or otherwise attributable to a State, conducted secretly, under disguise or false pretenses, and without

[48] Gayken, Sandro; Aitel, Dave. *What do policy-makers have to know about offense? (*2017 NATO CCD COE, unpublished material*)*
[49] Casey-Maslen, S., Corney, N. and Dymond-Bass, A. 'The review of weapons under international humanitarian law and human rights law', in Casey-Maslen, Stuart, ed. *Weapons under international human rights law* (Cambridge University Press, 2014), xv.
[50] Schmitt, n 9, 168.

> the (presumed) consent or approval of the owners or operators of the targeted IT-systems or computer networks or of the territorial State.[51]

In his book *Cyber Espionage and International Law* Russell Buchan defines cyber espionage as the use of cyber operations to copy confidential data that is resident in or transiting through cyberspace, even if it is not read or analysed. According to him, cyber espionage does not affect the availability or integrity of data or the networks and systems on which that data resides, and is conducted without the consent of the owners of the data.[52] Cyber espionage is, therefore, a broad enough term to accommodate any activity that aims to collect data on the target of a planned cyber attack.

Let us consider an alternative to the scenario from the *Tallinn Manual*.[53] State A is building a cyber capability that targets and is ultimately designed to disrupt the military communication networks of State B. The networks are connected to civilian systems. Since it is capable of impairing critical (information) infrastructure, the capability holds the potential to cause destruction amounting to a cyber attack and therefore qualifies as a cyber weapon. The weapon is designed to independently distinguish military communications from civilian ones. To do that, it first monitors and stores vast amounts of both civilian and military communications data. It gains unauthorised access to the public and private networks of State B, and installs spyware that sends both raw and analysed data to its operators. The software self-learns to distinguish strategic military from civilian data and draws conclusions on the patterns of life characteristic of a certain urban or rural environment in State B. Neither the service-providers nor the users are aware of such large-scale interceptions.

This kind of data exploit can be seen as an equivalent of Duqu or the first stages of Stuxnet. The main difference, which lends human rights its relevance, is that the spyware collects and analyses, not information about the functioning of a programmable logic controller, but the personal data of real individuals. Therefore, if the spyware with the self-learning module is deemed an integral part of the cyber capability, the capability infringes the privacy of regular users whose data is stored in or transmitted through the monitored networks. An alteration of the scenario which would eliminate the extraterritoriality conundrum would be if State A employed a similar program on its own networks to study the communications and geographic location of a separatist group. A different legal scenario would present itself, depending on whether the interception would take place during peacetime or a time of armed conflict. Here it is worth noting that the idea of weaponised intelligence is not a mere dystopian abstraction. According to unofficial sources, there are already precedents of 'weapons-grade' surveillance and data analysis technologies: namely, allegedly, the very algorithms that lied behind the Cambridge Analytica scandals in 2017 were originally developed for information warfare purposes and subjected to export control by the British government.[54]

The majority of cyber weapons are developed and their non-disruptive capabilities employed during peacetime, and so the extent to which weapons reviews should consider peacetime laws is particularly relevant. While espionage is said to reside in the heart of the grey area of public international law, it is subject to certain limits and conditions that are derived from ratified treaties and affirmed by international courts. Practices of espionage have been on trial several times and case law has determined the limitations, essential guarantees and remedies that have to be in place to ensure the fundamental rights

---

[51] Ziolkowski, Katharina, *Peacetime regime for state activities in cyberspace* (Tallinn: NATO CCD COE Publications 2013), 429.
[52] Buchan, Russell, *Cyber Espionage and International Law* (Hart 2018), 17.
[53] At p 3.
[54] *See e.g.*: Bryant, Emma L.'As Cambridge Analytica and SCL Elections shut down, SCL Group's defence work needs real scrutiny' OpenDemocracy (4 May 2018) https://www.opendemocracy.net/en/opendemocracyuk/as-cambridge-analytica-and-scl-elections-shut-down-scl-groups-defence-work-needs-re/ .

compliance of an intelligence-gathering measure. When we endorse Lewis's view of cyber attacks as weaponised signals intelligence,[55] existing case law on intelligence gathering and especially untargeted surveillance serve as a compass.

US SIGINT programmes such as PRISM, TEMPORA and UPSTREAM have been well-documented and while only five states in Europe have admitted to having the capacity and framework in place for conducting untargeted surveillance,[56] the main avenue for such practice was underpinned by the obligation for telecom service providers to retain communications metadata for, *inter alia*, national security and law enforcement purposes. The practice has, however, been ruled illegitimate by the European Court of Justice. Intelligence methods of various kinds have been adjudicated by the European Court of Human Rights, and most recently it has issued judgements on untargeted signals intelligence cooperation programmes in the UK[57] and Sweden.[58] While not as unforgiving towards bulk surveillance as the CJEU, the ECtHR has also come up with a set of fundamental standards and safeguards that an intelligence measure has to meet.

The following is a slightly Eurocentric analysis of how IHRL's regulation of intelligence activities might influence the procedure of cyber weapons reviews and does not necessarily reflect the norms of customary IHRL. First, any infringement of privacy caused by an intelligence measure must be explicitly prescribed by law and limited to those strictly and demonstrably necessary to achieve a legitimate aim. Second, the intelligence gathering has to serve a legitimate aim such as fighting serious crime or ensuring national security. In the context of a cyber weapon, a very probable legitimate aim for collecting bulk civilian data would be to improve the capacity to distinguish between military and civilian objects during a forthcoming cyber attack and thus minimise damage. Third, any measure has to be necessary and proportionate, which implies that, before turning to an intelligence measure, it has to be established that:

1) There is a high degree of probability that a serious crime or act(s) amounting to a specific serious threat has been or will be carried out.
2) Data relevant to the legitimate aim will be collected by employing the selected intelligence measure.
3) There are no other less intrusive ways to collect the relevant data.

The ECtHR[59] and CJEU[60] have elaborated on these requirements and derived a 'minimum safeguards against abuse' test that elaborates the classical threefold approach, breaking it down to eight elements.[61] First, the law that legitimises the surveillance measure has to be sufficiently clear and accessible. Secondly, the scope of application of the surveillance measure has to be specified. This implies that the nature of the offences and the legitimate aim have to be spelt out. No measure can be applied for an unlimited period. The ECtHR foresees that a European Convention on Human Rights (ECHR)-compliant surveillance regime has to include well-regulated access procedures, prior authorisation, independent

---

[55] Lewis, n 4.
[56] EU Agency for Fundamental Rights (FRA), Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal Update (2017), https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu
[57] *Big Brother Watch v UK* App nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018).
[58] *Centrum för Rättvisa v. Sweden,* App no. 35252/08, (ECtHR, 19 June 2018).
[59] Centrum för Rättvisa v. Sweden, App no. 35252/08, 19 June 2018; Big Brother Watch v UK App nos. 58170/13, 62322/14 and 24960/15, 13 September 2018.
[60] CJEU, Joined Cases C-203/15 and C-698/15 of Tele2 and Watson, 21 December 2016; Joined Cases C-293/12 and C-594/1 Digital Rights Ireland, 8 April 2014
[61] *See also*: Plixavra Vogiatzoglou, 'Bulk interception of communications in Sweden meets Convention standards: the latest addition to mass surveillance case law by the European Court of Human Rights', Strasbourg Observers (9 July 2018) https://strasbourgobservers.com/2018/07/09/bulk-interception-of-communications-in-sweden-meets-convention-standards-the-latest-addition-to-mass-surveillance-case-law-by-the-european-court-of-human-rights/.

oversight, obligation of notification of the surveillance and effective remedies for victims of privacy violations. It also has to lay down conditions for communicating the intercepted data to other parties, including the intelligence agencies of other states. The hypothetical cyber weapon described above fails to meet the minimum safeguards test, and therefore would be illegal in jurisdictions bound by ECHR or the EU Charter of Fundamental Rights, regardless of whether or not its ultimate effect amounts to a violation of IHL.

This should, perhaps, be reflected in weapons reviews, or there is a risk that a legal vacuum might arise where a cyber weapon is reviewed only as to whether or not its designed effects are in accordance with IHL, the cyber espionage component slipping under the radar. Brown and Metcalf, senior legal advisers to, respectively, US Cyber Command and the US Marine Corps Cyberspace Command have expressed concerns that 'an overly broad definition [of a cyber weapon] could encompass espionage tools and techniques, subjecting that area to unprecedented and unnecessary scrutiny would disrupt operations vital to national security'.[62] Through the lens of IHRL, the scrutiny seems anything but unnecessary. States are known for having as diverse, isolated and often incompatible procedures for weapons reviews as they do for intelligence oversight. The main problem is that, without knowing how IHL and IHRL interact in the realm of cyber weapons review, it would be easy for States to go context shopping and pick the framework that best suits their strategic and political objectives, but which does not ensure a meaningful legal review. This might allow a weapon which, while not inherently indiscriminate or of a nature to cause superfluous injury or unnecessary suffering, violates IHRL during peacetime, to pass an Article 36 review.

Tallinn Manual group of experts stresses that Article 36 requires the review to address whether employment of the means or method will comply with international law generally, not only the law of armed conflict[63]. Also, some traces in the *travaux préparatoires* of AP I are pointing in the same direction. Australia, Finland, the Netherlands and Sweden suggested amending the text of Article 36 so that it would be limited to ensuring compliance with IHL. However, the proposed limitations were not adopted and a broader scope was preferred in the final text of the Protocol.[64] In the debates surrounding (lethal) autonomous weapons systems, States are still considering whether the notion of applicable legal framework entails IHRL.[65] By contrast, there is little if any disagreement on the applicability of international humanitarian law.

When one is to accept that compliance with international law entails observing the rules of IHRL, then another question naturally emerges: whether we should be guided by IHRL as it applies during armed conflict or peacetime. This has significance, since privacy in IHL is an unmapped territory sometimes perceived as a non-issue, while in peacetime it is deemed a prerequisite to dignity and personal autonomy. Assuming that the aim of the hypothetical cyber weapon is better targeting during a conflict, this should be weighed against other values at stake. Therefore, if large quantities of civilian data are being collected and analysed during peacetime to improve targeting capabilities during a future armed

---

[62] Brown, G.D. and Metcalf, A.O., 'Easier said than done: legal reviews of cyber weapons.' *J. Nat'l Sec. L. & Pol'y*, *7* (2014), 115.
[63] Tallinn Manual, 465.
[64] Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva (1974–1977), Conference doc. CDDH/III/226, (25 February1975).
[65] Lewis, Dustin A., 'Legal reviews of weapons, means and methods of warfare involving artificial intelligence: 16 elements to consider', ICRC blogs (21 March 2019) https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/ .

conflict, the review should go further than ensuring compliance with IHL and should apply the abovementioned requirements and safeguards laid down by IHRL.

As for the legitimate aim requirement, the ECtHR has resisted interpreting the legal grounds for privacy infringements too broadly. In *Ekimdzhiev*, it declined to expand the concept of national security beyond its natural meaning.[66] Throughout its jurisprudence, the ECtHR has accepted as threats to national security: armed attack;[67] espionage;[68] terrorism and the incitement or approval of terrorism;[69] and separatist extremist organisations that threaten the unity or security of a state by violent or undemocratic means.[70] The Court has not ruled out strategic or anticipative surveillance in its entirety, provided that the absence of a firm evidence-based suspicion is necessary and compensated by sufficient procedural safeguards.[71] As cyber capabilities are tailor-made and not developed to be stored on a shelf in case a need might arise, the test of necessity would involve some sound pondering on the likelihood of the particular armed conflict occurring in the first place. Only if it is estimated to be sufficiently high should it be considered, if there are other less infringing tactics to improve the targeting function. If bulk surveillance indeed proves to be the most efficient measure, it should be ensured that no more data is stored than is necessary for the legitimate aim and any surplus is properly deleted. To avoid function creep, data leaks, profiling and unwarranted surveillance, a strict regime of systematic deletion should be established.

There are also some IHRL standards that are particularly difficult and in some cases unfeasible to impose. For instance, data subjects should be notified about the collection and use of their personal data. Understandably, the requirement of notification could hardly ever be enforced in the development of a cyber weapon. After the weapon has achieved its effect, the legal framework is likely to have shifted from peacetime to IHL, which deprives the duty to notify of much of its significance. As for effective remedies, if the planned cyber operation does not take place, yet the collected data is not deleted and is used for another purpose, the data subjects have the right to file appeals and receive compensation. The right, however, is likely to prove an onerous one to exercise since both intelligence and weapons oversight are veiled by confidentiality. All the safeguards and remedies are dependent on a regime of efficient and qualified oversight, which is why it should be established whether developing an espionage-heavy cyber capability falls within the competence of the weapons review or intelligence oversight body.

Weapons reviews vs intelligence oversight – different procedures and values applied to the same object

Just like any intelligence operation, data collection that has been built into a cyber capability should be systematically reviewed by an independent authority. In practice, this requirement might prove problematic, since, first of all, it is unclear whether the task should be fulfilled by the intelligence overview body or the one responsible for the review of the particular weapon. Ideally, a mutually complementary cooperation model could be established between two of the most secretive communities that may or

[66] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, App no. 62540/00 (28 June 2007), para 84.
[67] *Weber and Saravia v. Germany*, no. 54934/00, (29 June 2006),
[68] *Roman Zakharov v. Russia*, no. 47143/06 (4 December 2015).
[69] *Zana v. Turkey*, no. 69/1996/688/880, (25 November 1997).
[70] *United Communist Party of Turkey v. Turkey*, App No 19392/92 (30 January 1998).
[71] *Weber and Saravia v. Germany*, n 59; *Big Brother Watch v. UK*, App nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018).

may not have developed a model for information sharing. Procedural and technical obstacles aside, intelligence oversight institutions are best placed to assess the human rights compliance of any intelligence operation, including the ones integrated into a cyber capability. Any opinion given by a competent oversight body should, therefore, affect the overall legal review of a cyber weapon.

Both intelligence oversight and weapons review are highly classified procedures that are carried out by different institutions with different values, cultures and objectives. Despite the generally disguised nature, after the Snowden revelations in 2013 there was a dramatic surge in public interest and consequently also research into the workings of intelligence agencies and how they can be overseen. As of today, weapons reviews are yet to go through an equivalent revolution in transparency. Intelligence oversight is process-oriented, continuous, dispersed and centres on accountability: the main purpose of oversight is to hold intelligence services to account for their policies and actions in terms of legality, propriety, effectiveness, and efficiency.

According to Ian Born and Aidan Wills, accountability is best understood as a process of account giving and account holding that takes place within an established relationship. In this relationship, the intelligence service (or individual within that service) is the account giver, who can be obligated to render account to the overseer, which has the right to demand such account. Born and Wills list the four components of accountability: 1) the intelligence services or their officers that are held to account; 2) the institution to which they give account (the overseer); 3) the areas of intelligence work that are subject to accountability; and 4) the legal, financial, resource and expert capacity of the overseer to hold intelligence services accountable for international intelligence cooperation.[72] Weapons reviews, by contrast, direct their focus towards minimisation of damages and precaution.

The intelligence cycle usually comprises five steps: (1) planning and direction; (2) collection; (3) processing; (4) production and analysis; and, (5) dissemination.[73] Each of these steps can be executed through cyber means and also, increasingly, in an automated or autonomous manner. A similar intelligence cycle has been laid out by the national government (Rijksoverheid) of the Netherlands. Ideally, oversight should extend to each of these phases. The most advanced models of intelligence oversight combine parliamentary, judiciary, executive and expert oversight and cover *ex ante*, ongoing and *ex post* phases.[74] The institutional framework for intelligence oversight tends to be complex and consist of several different administrative oversight bodies.[75] Australia, Germany, the Netherlands, the US and the UK are among the states where the intelligence oversight and weapons review regimes have been relatively widely documented, but in none do the entities responsible for intelligence oversight even partially overlap with those coordinating weapons reviews (see Table 1). Ostensibly, therefore, the two communities operate separately and are in no way obliged to engage in information or expertise sharing.

---

[72] Born, H., Leigh, I. and Wills, A., 'Making international intelligence cooperation accountable', (DCAF-The Geneva Centre for the Democratic Control of Armed Forces, 2015), 7.
[73]Aidan Wills, 'Guidebook: Understanding Intelligence Oversight', (Geneva Centre for the Democratic Control of Armed Forces, 2010), 36.
[74] EU Agency for Fundamental Rights (FRA), Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update (FRA, 2017), https://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-legal
[75] Ibid.

TABLE 1

	Weapons Review[76]	Intelligence Oversight[77]
Australia	Directorate of Operations and Security Law, Defence Legal, Department of Defence	Inspector-General of Intelligence and Security, Parliamentary Joint Committee on Intelligence and Security
Germany	Steering Group for the Legal Review of New Weapons and Methods of Warfare, Federal Ministry of Defence	G 10 Commission; Parliamentary Control Panel
The Netherlands	Advisory Committee on International Law and the Use of Conventional Weapons	Intelligence and Security Review Committee (CTIVD), Committee on the Intelligence and Security Services; Committee in the Interior
United Kingdom	MOD Development Concepts and Doctrine Centre	Investigatory Powers Tribunal; Intelligence and Security Committee; Interception of Communications Commissioners; Intelligence Services Commissioner;
USA	Office of the Judge Advocate General of the respective service (Navy/Army/Air Force/…)	Inspector General FBI, Inspector General CIA, Inspector General NSA, Inspector General NGA, Inspector General for the Intelligence Community, Senate Select Committee on Intelligence, House Committee

Unlike intelligence oversight, weapons reviews are intended to solve a particular one-off issue through active inquiry and do not entail continuous scrutiny. However, the efficiency of a typical weapons review procedure in the context of new weapon technologies has been questioned multiple times[78]. For sophisticated cyber weapons that are to a large extent dependent on uninterrupted data exploits, a supervisory framework similar to that of intelligence oversight would be better suited. In 2015 the Council of Europe Commissioner for Human Rights issued a paper on democratic and effective oversight of national security services, in which it was stated that external authorisation should, among other intelligence activities, extend to untargeted bulk collection of information, use of keywords or selectors to extract data from the information and collection of and access to communications data (including when held by the private sector).[79] These categories are likely to form the basis of an advanced custom-

[76] PREMT - Program on the Regulation of Emerging Military Technologies, Legal Reviews of Weapons, https://www.premt.net/resources/legal-review/.
[77] See e.g: Leigh I, Wegge N (eds), *Intelligence Oversight in the Twenty-first Century: Accountability in a Changing World*, (Routledge, 2018).; Richardson S, Gilmour N. *Intelligence and Security Oversight: An Annotated Bibliography and Comparative Analysis* (Springer, 2016), 37 – 41.
[78] See eg: ICRC, 'International humanitarian law and the challenges of contemporary armed conflicts', (2019), 29, https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf.
[79] Aidan Wills, 'Democratic and effective oversight of national security services', (Council of Europe Commissioner for Human Rights, 2015), 15.

made cyber capability and as spelt out, for instance, in the white paper on weapons reviews in the UK, might become the object of a weapons review.[80]

If the review of advanced cyber capabilities were to borrow from the best practices of intelligence oversight, it would, at least in States that are bound by ECHR or EU Charter of Fundamental Rights, connote that the data exploits should comply with certain standards. First, they should be subject to prior authorisation. In *Zakharov vs Russia*, the ECtHR held that a number of factors determine whether secret surveillance has not been ordered haphazardly, irregularly or without due and proper consideration. Among these factors, the Court attributed particular importance to the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation.[81] In addition, the Court highlighted the importance of the substance and quality of the *ex ante* review in circumstances where the individual is necessarily prevented from seeking an effective remedy.[82] Therefore, the data exploits built into a cyber capability should also be reviewed by a technically and legally competent oversight body before, during and after their deployment and this should cover all surveillance processes from collection to destruction of the data.

The United Nations High Commissioner for Human Rights has reiterated the importance of the oversight bodies being independent of the ones authorising and applying surveillance measures.[83] This would imply that the body responsible for reviewing an espionage-based cyber weapon would have to be independent of the one authorising its procurement and use. This requirement would apparently be overruled in cases where weapons reviews are conducted within the same institutional unit (e.g. Ministry of Defence), that is responsible for development or procurement and the subsequent use of military equipment. This is another reason why Article 36 reviews should be conducted by, or in close cooperation with, intelligence oversight bodies.

Intelligence oversight frameworks have long been criticised for being under-resourced, lacking in expertise in technical matters and not having any real power to mitigate privacy violations.[84] However, in its comprehensiveness intelligence oversight still proves better suited for the scrutiny and assessment of peacetime data collection than a weapons review framework. Article 36 was not drafted with cyber capabilities in mind, and when one is to search for other weapons that could operate in a latent manner during peacetime, only land mines come to mind. While atrocious and destructive, land mines, however, are, a poor analogy since they are passive unless activated by their victim.

While the text of Article 36 is not unequivocally closing the door to reviewing new weapons, means or methods or warfare according to peacetime IHRL, based on the currently prevalent comments and interpretations, intelligence oversight and weapons reviews tend to be kept apart. One way is to see data exploits as integral parts of a cyber capability. This would imply that the capability is deployed during peacetime and should be assessed pursuant to IHRL standards on intelligence gathering by an oversight body best suited for it. Alternatively, while often technically infeasible, it can still be argued that the data exploits are strictly separate from the deployment. This would in fact lead to the same result – when we view peace as the normality and war as the exception, all surveillance should adhere

---

[80] UK, Ministry of Defence, UK Weapon Reviews, 4, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/507319/20160308-UK_weapon_reviews.pdf.
[81] *ECtHR, Roman Zakharov v. Russia*, no. 47143/06 (4 December 2015), para 257.
[82] Ibid, para 233.
[83] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018), paras 39-40, https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx .
[84] FRA, n 66.

to IHRL rules on legality, necessity and proportionality. When a cyber espionage program fails to do so, the capability that it is meant to support should (and, indeed, could) not be deployed.

Conclusion

As there are few, if any, weapons, means or methods of warfare as silent and slow as a sophisticated cyber capability, analogies only go a short way. The principal argument of the working paper could be summarised by a simple question: should a weapon that can only come to existence as a result of systematic human rights violations during peacetime be deemed legal, provided that it does not violate IHL during armed conflict? If we put the same question in the context of the right to life, the prohibition of torture and inhuman treatment or freedom of expression, the collective reply would likely be in the negative. But the question does not make sense in any of these contexts. It is, at least as for now, specific to the right to privacy, surveillance and cyber operations and capabilities. Even though there are no known real-life examples of cyber weapons that have contained an element of mass surveillance, given the current technological backdrop of machine learning, data mining, big data analysis, interoperable solutions for smart cities and digitalised public services, the available data on life patterns is too abundant and valuable not to be used for military purposes. In essence, this has no immediate negative connotations, indeed the availability of precise and dynamic civilian data might result in better targeting and fewer casualties.

It might also prove technically impossible and strategically infeasible to dissect the parts of software that are designed to extract and analyse data from the whole of the cyber capability. Therefore, the deployment of the capability can be perceived to take place as soon as the software enters the target, usually during peacetime. Alternatively, when the circumstances justify separating the use of the cyber capability from the espionage, the latter ends up forming an essential part of the development procedure. Either way, Article 36 and available prevailing state opinion seem to support conducting legal reviews at the earliest possible stage during the development phases of a new capability. This aspect seems to bear particular importance for certain cyber capabilities where consideration of the applicability of Article 36 is strictly linked with the effects created by the weaponised code. Such technologies are characterised by an atypical development process where the conceptual and design processes of the early stages are strongly linked to the final use of the capability. Therefore, when a capability collects and processes data to support the foreseen final effects, the espionage component within the capability needs legal consideration under Article 36.

The Australian example of a multi-stage review is just one example of how States are responding to the new challenges derived from the atypical life cycle of cyber capabilities. Dividing the final review in interim considerations of Article 36 not only reflects the atypical development of certain cyber capabilities, but also shows a causal link between the various phases of the development of a cyber capability. Although the obligation stemming from Article 36 applies to weapons, means and methods of warfare and it is yet to be clarified into which of these categories a certain cyber capability would fall, the application of Article 36 might need to be considered even before a capability acquires such a label. Therefore, the correct timing to consider the expected effects of new technologies that are weaponised and tailor made for specific purposes would fall within the study process of new cyber capabilities.

When the early effects infringe the privacy of civilians during peacetime, they should be evaluated under IHRL based on its proportionality, necessity and legality. The current regime of weapons reviews is poorly equipped for the task and should borrow its *mod*us *operandi* and legal standards from the best practices of independent intelligence oversight bodies. In states that are bound to the ECHR, the integrated espionage modules of such cyber capabilities should follow the case law of ECtHR. This

would require that the cyber capability can only be deployed or developed provided that the prior data collection has had a legitimate aim and follows the principles of necessity, legality and proportionality. This would imply that large-scale monitoring on any group of individuals for strategic or preventive purposes without being able to demonstrate a national security purpose would not be permitted. In cases where strategic monitoring incorporated in a cyber capability has proved vital, it has to be backed up by sufficient guarantees, remedies and independent oversight.

Traditionally, weapons reviewers have not operated in these terms and, while displaying some weaknesses of their own, intelligence oversight bodies seem to be better positioned to oversee the legality of peacetime cyber espionage and therefore decide on the legality of a cyber capability. In conclusion, the paper argued that weapon which contains an integral element of excessive collection of civilian data during peacetime should not be deemed legal according to IHRL and Article 36 of AP I to the Geneva Conventions. This is far from marking the end of the issue; rather, it raises new questions about the classification of cyber capabilities, extent and sources of the obligation to review new weapons, means or methods of warfare, privacy and cyber espionage during armed conflict and the timeframe of effective oversight.

References

Treaties

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1125 U.N.T.S. 3 (June 8, 1977).

Cases

European Court of Human Rights

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App no. 62540/00 (28 June 2007).

Centrum för Rättvisa v. Sweden, no. 35252/08 (19 June 2018).

Roman Zakharov v. Russia, no. 47143/06 (4 December 2015).

Klass and Others v. Germany, no. 5029/71 (6 September 1978).

Weber and Saravia v. Germany, no. 54934/00, (29 June 2006).

Big Brother Watch v UK App nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018).

Zana v. Turkey, no. 69/1996/688/880, (25 November 1997).

United Communist Party of Turkey v. Turkey, App No 19392/92 (30 January 1998)

Court of Justice of the European Union

Joined Cases C-203/15 and C-698/15 of Tele2 and Watson (21 December 2016)

Jolned Cases C-293/12 and C-594/1 of Digital Rights Ireland (8 April 2014)

Documents

Australia, 'The Australian Article 36 Review Process' (30 August 2018) UN Doc CCW/GGE.2/2018/WP.

Argentina, Streng thening of the review mechanism of a new weapon, means and method of warfare - Working Paper Drafted by Argentina, CCW/GGE.1/2018/WP.2, page 3. (http://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/documents/GGE.1-WP2-English.pdf).

Denmark, Royal Danish Defense College, Joint Doctrine for Military Cyberspace Operations, (September 2019).

The Netherlands and Switzerland, 'Weapons Review Mechanism' (7 November 2017) UN Doc CCW/GGE.1/2017/WP.5. 'Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects' (15 November 2019) UN Doc CCW/MSP/2019/CRP.2/Rev.1, Annex III.

Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Geneva (1974–1977), Conference doc. CDDH/III/226, (25 February 1975).

United States Air Force, Legal Reviews of Weapons and Cyber Capabilities, A.F. INSTRUCTION 51-402 (July 27, 2011), https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-053.pdf .

Other Sources

Boldizsár Bencsáth, Gábor Pék, Levente Buttyan and Mark Felegyhazi, 'The Cousins of Stuxnet: Duqu, Flame, and Gauss, (2012) *Future Internet* 4(4) 975.

Emma Bryant, 'As Cambridge Analytica and SCL Elections shut down, SCL Group's defence work needs real scrutiny' OpenDemocracy (4 May 2018) https://www.opendemocracy.net/en/opendemocracyuk/as-cambridge-analytica-and-scl-elections-shut-down-scl-groups-defence-work-needs-re/.

Jeffrey T. Biller and Michael N. Schmitt, 'Classification of cyber capabilities and operations as weapons, means, or methods of warfare', *(2019) 95 International Law Studies*.

P.J. Blount, 'The preoperational legal review of cyber capabilities: Ensuring the legality of cyber weapons' (2012) *N. Ky. L. Rev 39*.

William Boothby, *Weapons and the Law of Armed Conflict* , (Oxford University Press, 2016).

William Boothby, 'How Will Weapons Reviews Address the Challenges Posed by New Technologies' (2013) *52 Mil L & L War Rev 37*.

Gary Brown and Andrew Metcalf, 'Easier said than done: legal reviews of cyber weapons.' (2014), *J. Nat'l Sec. L. & Pol'y 7.*

Russell Buchan, *Cyber Espionage and International Law* (Hart, 2018).

Stuart Casey-Maslen, Neil Corney and Abi Dymond-Bass, 'The review of weapons under international humanitarian law and human rights law', in Stuart Casey-Maslen, ed. *Weapons under International Human Rights Law* (Cambridge University Press, 2014).

Stuart Casey-Maslen and Tobias Vestner, *A Guide to International Disarmament Law* (Routledge, 2019),

EU Agency for Fundamental Rights (FRA), *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update* (FRA, 2017) https://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-legal.

Sandro Gayken, Dave Aitel, 'What do policy-makers have to know about offense?' (2017 NATO CCD COE, unpublished material).

Mark Gibbs, 'Why Stuxnet is a really bad weapon' *NetworkWorld*, (22 June 2012) https://www.networkworld.com/article/2189571/why-stuxnet-is-a-really-bad-weapon.html

Sue Halpern, 'How cyber weapons are changing the landscape of modern warfare', *New Yorker* (18 July 2019)

ICRC, 'International humanitarian law and the challenges of contemporary armed conflicts', (2019), 29, https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf.

Infosec, 'The Rise of Cyber Weapons and Relative Impact on Cyberspace', (5 October 2012) https://resources.infosecinstitute.com/the-rise-of-cyber-weapons-and-relative-impact-on-cyberspace .

Ralph Langner, 'Stuxnet: Dissecting a cyberwarfare weapon' (2011) 9 *IEEE Security & Privacy Magazine* 49.

Dustin A. Lewis, 'Legal reviews of weapons, means and methods of warfare involving artificial intelligence: 16 elements to consider' ICRC blogs (21 March 2019) https://blogs.icrc.org/law-and-policy/2019/03/21/legal-reviews-weapons-means-methods-warfare-artificial-intelligence-16-elements-consider/

James A. Lewis, 'In defense of Stuxnet' *Military and Strategic Affairs* 4, no. 3 (2012) 65-76, 66.

Herbert Lin and Amy Zegart, eds. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Brookings Institution Press, 2019).

Justin McClelland, 'The review of weapons in accordance with Article 36 of Additional Protocol I'. *International Review of the Red Cross* 85, no. 850 (2003).

Robert McMillan, 'Siemens confirms German customer hit by Stuxnet espionage worm') *InfoWorld*(21 July 2010) https://www.infoworld.com/article/2625529/siemens-confirms-german-customer-hit-by-stuxnet-espionage-worm.html.

Thomas Rid and Peter McBurney. 'Cyber-weapons' *The RUSI Journal* 157, 1 (2012).

Michael N. Schmitt. (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017)

Plixavra Vogiatzoglou, 'Bulk interception of communications in Sweden meets Convention standards: the latest addition to mass surveillance case law by the European Court of Human Rights', Strasbourg Observers (9 July 2018) https://strasbourgobservers.com/2018/07/09/bulk-interception-of-communications-in-sweden-meets-convention-standards-the-latest-addition-to-mass-surveillance-case-law-by-the-european-court-of-human-rights/.

David Wallace, 'Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis' (2018) Tallinn Paper no 11.

Aidan Wills, 'Democratic and effective oversight of national security services', (Council of Europe Commissioner for Human Rights, 2015).

Aidan Wills, 'Guidebook: Understanding Intelligence Oversight', (Geneva Centre for the Democratic Control of Armed Forces, 2010).

Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace* (Tallinn: NATO CCD COE Publications 2013).