Cyber War Has Indeed Not Taken Place! – Yet?

AUTHOR
Mercedes Abdalla

ABSTRACT
The concept of ‘cyber warfare’ has become one of those buzz words that prominently feature in the political and public discourse. As it been similarly widely ‘abused’ in the media. Despite it being a term that speaks to the imagination, in essence, it is a more complex phenomenon, which desires in-depth scrutiny in order to distill the current conceptual muddle surrounding the notion. Nonetheless, a divergence in opinion within the academic debate is likewise present as to whether cyber space has become the fifth domain of warfare on par with air, sea, land and space. While some suggest, ‘cyber war is inevitable’ and that ‘cyber-attacks can in fact be construed as acts of war’, other scholars reject the idea and argue that neither have cyber capabilities become a ‘new absolute’ weapon of cyber warfare nor cyber war has and will ever take place (McGraw, 2013; Stone, 2013; Liff, 2012; Rid, 2012). These differing assumptions have been proclaimed on the basis of varying analytical discourses examining the theoretical linkage between cyber activities and warfare. The concept has been extensively studied across disciplines such as international relations, military philosophy and strategic studies, to name only a few. This, has inevitably resulted in the absence of a clear understanding what cyber-attacks are and whether they can be regarded as acts of war.

Correspondence Address
Mercedes Abdalla, MSc Candidate, University of Leiden, Netherlands.
Email: Mercedes.abdalla@gmail.com

INTRODUCTION
The concept of ‘cyber warfare’ has become one of those buzz words that prominently feature in the political and public discourse. As it been similarly widely ‘abused’ in the media. Despite it being a term that speaks to the imagination, in essence, it is a more complex phenomenon, which desires in-depth scrutiny in order to distill the current conceptual muddle surrounding the notion. Nonetheless, a divergence in opinion within the academic debate is likewise present as to whether cyber space has become the fifth domain of warfare on par with air, sea, land and space. While some suggest, ‘cyber war is inevitable’ and that ‘cyber-attacks can in fact be construed as acts of war’, other scholars reject the idea and argue that neither have cyber capabilities become a ‘new absolute’ weapon of cyber warfare nor cyber war has and will ever take place (McGraw, 2013; Stone, 2013; Liff, 2012; Rid, 2012). These differing assumptions have been proclaimed on the basis of varying analytical discourses examining the theoretical linkage between cyber activities and warfare. The concept has been extensively studied across disciplines such as international relations, military philosophy and strategic studies, to name only a few. This, has inevitably resulted in the absence of a clear understanding what cyber-attacks are and whether they can be regarded as acts of war.

This essay seeks to add to this conceptual debate and approach the phenomenon through the lens of legality. In doing so, it will resort to the legal framework offered by the Tallinn Manual. The fundamental premise of the Manual is that international law does apply to the cyber domain. The Tallinn Manual aims to distill the applicability of international law of armed conflict to the conduct of defensive and/or offensive activities in the cyber realm and set out the governing Rules thereof. Nonetheless, the purpose of this paper is neither to test this assumption nor
to reflect upon the jus ad bellum and the jus in bello as applied to cyber warfare. Instead, it aims to utilize the legal conceptualization of the terms ‘international armed conflict’ and ‘cyber-attack’ as outlined in the Manual in order to determine when cyber-attacks account for acts of war.

The essay will follow a two-fold structure; first it will outline those ‘black-letter-rules’ of the Manual that shed light on the warlike nature of cyber-attacks. To provide an answer to the question as to ‘whether cyber war has taken place in recent years?’, cyber-attacks, as acts of war – using the Manual’s understanding – will be applied to two specific case studies:

1. The hacking targeted against Georgia during its military confrontation with Russia in 2008 will be examined.
2. Followed by a more recent event considering the ongoing political and military conflict between the Russian Federation and Ukraine. In this setting, the cyber incident that occurred at the Ukrainian power plant in 2015 will be analysed. In this vein, it is important to emphasize that these instances were not the only ones in which conducted cyber activities constituted substantial threat to a state’s national security.

However, both cases took place in the setting of a de jure international armed conflict. They, therefore, provide fruitful cases for analysis to determine whether cyber-attacks, as acts of war have already been witnessed in modern warfare.

**THE TALLINN MANUAL**

The first version of the Tallinn Manual on Cyberwarfare was published in 2013 by a group of independent legal practitioners and scholars at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence. It is a non-binding academic document and to date it arguably represents one of the most comprehensive legal analyses on cyber warfare. In their attempt, the International Group of Experts – hereinafter referred to as experts – aimed to address the applicability of legal norms to cyber acts, as a newly arising form of irregular warfare; ‘in the hope of bringing some degree of clarity to the complex legal issues surrounding cyber operations’ (Schmitt, 2013). Hence, in doing so, the Tallinn Manual exclusively examines cyber activities as occurred in the conduct of an armed conflict, in the strict sense of cyber-to-cyber operations. As was discussed above, the primary aim of the Manual is to examine the justification of the resort to ‘cyber force’ by States as an instrument of their national policy and the legality of the conduct of ‘cyber warfare’ itself. Furthermore, it aims to clarify the legal denotation of cyber-attacks, as acts of war, embedding it into the context of an international armed conflict.

**RULE 22: CHARACTERISATION AS INTERNATIONAL ARMED CONFLICT**

A generally accepted legal understanding of an international armed conflict is based on Common Article 2 of the 1949 Geneva Conventions. As the Article provides, an internationally declared war or armed conflict exists between two or more states involved on opposing sides, ‘even if the state of war is not recognized by one of them’ (Schmitt, 2013). In addition to being international, an armed conflict also needs to fulfill the ‘armed’ component. Despite international law not specifying the exact meaning of ‘armed’, according to the commentary by the International Committee of the Red Cross on the 1949 Geneva Conventions, ‘any difference arising between two States and leading to the intervention of armed forces is an armed conflict’ (Schmitt, 2013). In the absence of a clear definition of ‘armed’ in international law, the Experts incorporated the notion of ‘hostilities’ in their Rule 22 on the ‘Characterization as international armed conflict’. They argue that ‘constituent hostilities may involve any combination of kinetic and cyber operations, or cyber operations alone’ (Schmitt, 2013). Moreover, they claim that ‘hostilities exist whenever one State engages in ‘cyber attacks’ against another’ (Schmitt, 2013).

**RULE 30: DEFINITION OF CYBER-ATTACKS**

The question follows; what does a cyber-attack entail de jure? In its Rule 30 on the ‘Definition of cyber-attack’, the Experts embed the meaning of the term in the legal understanding of ‘acts of violence’ as settled in the law of armed conflict. In this respect, to classify an act as a violent one, it does not solely need to pertain to the release of kinetic force. In other words, an attack – in the broader sense of the word – shall not be understood only in physical terms, but rather in terms of the effects it causes.

The Experts justify this argument on the articles of Additional Protocol I; while Article 51...
of the Protocol claims that civilian populations shall enjoy protection against the dangers arising in armed conflicts, the rules of proportionality address the ‘loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof’ (Schmitt, 2013). Consequently, when applying this reasoning to cyber-attacks, it is not so much about the nature of the act per se, but the discussion rather revolves around the consequences a cyber activity brings about. ‘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’ states Rule 30 (Schmitt, 2013). Although cyber-attacks may not necessarily entail the direct release of kinetic force directed against a certain digital system, they still may entail destruction to objects or harm to individuals, qualifying such activities as attacks.

It is furthermore argued that ‘whenever an attack on data results in the injury or death of individuals or destruction of physical objects, those individuals or objects constitute the ‘object’ of the attack’, qualifying the cyber operation again as an attack (Schmitt, 2013). In their discussion, the Experts also agree that interference by cyber means into the functionality of objects – either if it necessitates the replacement of physical components or data restoration – also presupposes damage or destruction, hence it similarly entails consequential harm triggered by the attack.

CYBER-ATTACKS AS AN ACT OF INTERNATIONAL ARMED CONFLICT

Any cyber-attack can be considered an act of an international armed conflict if it has been executed in its context, conveys Rule 20 on the ‘Applicability of the Law of Armed Conflict’ on cyber operations. A prerequisite to this is that ‘there must be a nexus between the cyber activity and the armed conflict’ as the Experts note (Schmitt, 2013). However, digital attribution, that is ascribing the agency to an agent when it comes to computer network intrusions, has become one of the most challenging dilemmas, requiring the complex understanding of the how, the what, the why, and most importantly, the who (Buchanan & Rid, 2015). In the Manual’s Rule 20 and 22, the experts similarly reflect upon the problematic nature of unmasking the who and whether in fact a State authorized cyber incident (Schmitt, 2013). The experts conclude, that there is an existing nexus between a cyber-attack and an armed conflict in the context of an ongoing war, if it has been conducted under the ‘overall control’ of a state (Schmitt, 2013). To capture the meaning of a State’s ‘overall control’ concerning the hostilities committed potentially by a non-State actor in the context of an international armed conflict, the Experts draw a parallel with Article 8 of the Articles on State responsibility. Applying it onto cyber-attacks committed by groups subordinate to the State, an ‘overall control’ over such activities exist if a state – even if it has not issued specific orders – does have a role in planning, organizing and coordinating such actions (Schmitt, 2013).

Translating the propositions made by the Experts into the logic of war, international armed conflict exists provided it meets two prerequisite conditions. Firstly, it needs to unfold between two or more States, regardless if one of the parties involved does not recognize the state of war. Secondly, an international conflict can be characterized as ‘armed’ if there are ongoing hostilities, involving kinetic operations and, as the expert’s assert – cyber-attacks. A cyber-attack meets the threshold of being an act of international war if it brings about consequential damage and if there is a nexus between the cyber act and the international armed conflict itself. Considering the challenging nature of attribution in this respect, the Experts conclude that a cyber-attack construes an act of war if the involved state has a role in planning, organizing and coordinating it.

RUSSIAN-GEORGIAN WAR: DEFACEMENTS AND DDOS ATTACKS

The escalation of events between the Russian Federation and Georgia in August 2008 found its roots in the long-standing geostrategic confrontation between the two nations. Both the South Ossetia War in 1992 and the Abkhazian War the following year resulted in de facto territorial losses for Georgia, with two unrecognized pro-Russian governments in both regions. Tensions remained until the eruption of the conflict in the summer of 2008. On 7 August, Georgian troops initiated military shelling on the town of Tskhinvali located in South Ossetia, in response to alleged provocations of the South Ossetian separatist forces. A day later, Russian combat troops were deployed in the breakaway region and at the same time, a naval blockade was set up around the former Soviet republic, utilizing Russian naval forces. On 9 August 2008, Georgian president, Mikheil Saakashvili, began
full-scale mobilization and declared the state of war between Georgia and the Russian Federation (Kaska, Tikk, & Vihul, 2010).

The cyber operations in the context of the armed confrontation with Russia in 2008 were arguably one of the first cases in which an international conflict was preceded and accompanied by cyber offensives. The cyber intrusions Georgia experienced were primarily three-fold; they consisted of defacements of governmental as well as financial websites, the launching of Distributed Denial of Service (DDoS) attacks targeting mostly media and numerous private online platforms and the distribution of malicious software on public domains. Concerning the former, the visual appearance of several governmental and financial sites – such as the website of the then Georgian president, the National Bank and the Ministry of Foreign Affairs – was changed and replaced with pejorative imagery (Kaska et al., 2010). The DDoS attacks were targeted against websites both from the public as well as the private sector, including governmental and online media platforms, among others. In addition to this, various Russian-language blogs and forums spread a downloadable batch script – accompanied with how-to instructions – that was again aimed at paralyzing several Georgian websites. Even though the first DDoS attack targeted against the president’s website had already taken place, hence before the actual military confrontation, the peak of similar attacks of this nature as well as most the defacements unfolded during the Russian-Georgian military standoff (Kaska et al., 2010).

Despite significantly limiting both the Georgian government’s national and international information flow, it is difficult to determine whether the Georgian cyber event brought about any consequential damage in line with the reasoning of the Manual’s Rule 30. In their analysis, the Cooperative Cyber Defense Centre of Excellence (CCD COE) suggests, that ‘the main damage was in limiting the nation’s possibilities to distribute information about the ongoing military conflict’ while the ‘cyber incidents also affected the provision of public services’ (Kaska et al., 2010). Nevertheless, the CCD COE similarly concludes that neither is it possible to estimate the financial damage of the incident nor ‘the attack (had) a permanent or even a long-run devastating effect on the Georgian Internet infrastructure’ (Kaska et al., 2010).

The question of attribution was another problem of the cyber incidents. To date, there has been no conclusive proof presented as to who in fact was behind the cyber intrusions, despite the appearance of providing coordination and instructions. In line with Arbor Networks’ data traffic analysis, all the cyber incidents were observed to be globally outsourced, ‘suggesting a botnet (or multiple botnets) behind them’ (Kaska et al., 2010). Some of the command and control botnet servers used in the DDoS attacks, nonetheless, had their ties back in Russia. As Tikk, Kaska and Vihul argue the Russian-hacker community’s involvement is unquestionable, there is; however, no evidence on the Russian administration providing support or that it had a role in coordinating the hackers. The Kremlin’s potential participation in the digital intrusion can be endorsed only by circumstantial evidence rooted in speculation (Kaska et al., 2010).

In line with the Manual’s definition, is it feasible to label the cyber hostilities Georgia witnessed in its military standoff with Russia as cyber-attacks that constituted acts of war? Hardly so. Firstly, the DDoS attacks as well as the defacements did not cause injury or damage neither to individuals nor to objects. They also did not necessitate the restoration of data in the targeted digital system. Secondly, due to the absence of clear-cut attribution it is similarly unfeasible to establish a link between the Russian government and the digital incident at hand.

THE UKRAINIAN-RUSSIAN WAR: POWER GRID BLACKOUT

A few years later yet another conflict escalated on the edge of the so-called Russian sphere of influence. The internal Ukrainian turbulence resulting from the eruption of the violent Maidan Revolution and the subsequent ousting of the pro-Russian Yanukovich government was accompanied by a rather unexpected move from the Russian authorities; in early 2014, Kremlin-backed ‘little green men’ seized control over the Crimean Peninsula that was followed by the illegal proclamation of independence from Ukraine. A similar sequence of events unfolded in the Eastern part of Ukraine shortly after the annexation of Crimea; pro-Russian separatists occupied governmental buildings, calling for a similar referendum on independence. Despite the Russian leadership denying any involvement in the outset of the conflict, facts on the ground during time have appeared to somewhat ‘speak for
themselves’. According to the UN Human Rights Monitoring Mission in Ukraine, the Kremlin has been covertly sending its military advisors, ‘volunteer fighters’, munitions as well as heavy weaponry to assist rebels in their fight against the Ukrainian military. The Ukrainian, then-interim government rightfully regarded the Russian moves as infringement on Ukrainian sovereignty and declared war against the Russian Federation, which has never been met with the same rhetoric from the Kremlin (Gumuchian, Lee, & Wedeman, 2014). Despite Russia not acknowledging direct confrontation with the military forces of Ukraine, per international law, the current situation still accounts to an international armed conflict due to the ongoing hostilities between the two states.

In December 2015 Ukraine witnessed yet another ‘attack’ in its nature novel aggression, in the context of the ongoing conflict, due to a malicious hack a power outage occurred, leaving some 225 000 thousand customers without electricity for a few hours. This incident was the ‘first known successful cyber intrusion to knock a power grid offline’ and quickly became labeled as a ‘cyber-attack’ by the media and politicians alike (Volz, 2016). Some went further and characterized the disruption caused within the critical infrastructure as an illustrative example of Russia waging a cyber war against its Western neighbor (Greenberg, 2017). Can, however, the incident of the Ukrainian power grid be regarded as a cyber-attack and consequently, an act of war in the framework of the Russian-Ukrainian conflict?

First and foremost, in order to determine whether the Ukrainian power grid incident constituted a cyber-attack in line with the Tallinn Manual’s Rule 30, it is essential to examine the consequential damage it brought about. The intrusion prompting the power grid going offline was targeted against three electricity providers with a set of combined technical components, demonstrating the ‘highly synchronized, multistage, (and) multisite’ nature of the attack (Assante, Conway, & Lee, 2016). Access to business networks was acquired mainly through spear phishing. This as a whole, was responsible for the electricity malfunction. Despite not causing direct injury or destruction either to individuals or to the critical infrastructure in question, Rule 30’s characterization of a cyber-attack, interfering into the functionality of an object necessitating the restoration of the targeted object’s data is indeed applicable to this case. Did this cyber-attack, nonetheless, amount to an act of war in the framework of the Ukrainian-Russian confrontation?

Keeping in mind the prerequisite outlined by the Experts on the overall control of a State pertaining to any cyber-attacks, one could label the case of the power grid intrusion as an act of warfare provided it is definable that the Kremlin had a role in planning, organizing and coordinating it. As of this point, no substantial evidence has been presented that would justify this claim. Even though shortly after the attack investigations authorized by the Ukrainian energy ministry revealed that the hack was carried out using a Russian-based Internet provider, the Ukrainian authorities restrained from directly attributing it to the Russian government (Polityuk, 2016). In their analysis based on ‘sensitive sources’ U.S. cyber intelligence firm iSight Partners, moreover, concluded that the attack was linked to the Russian hacking group known as ‘Sandworm’, but they were unable to identify whether it was carried out under the direct planning, coordination and organization of the Russian government (Volz, 2016; Finkle, 2016). In the absence of a clearly defined attribution it can be hardly claimed that there was an existing nexus between this cyber-attack and the wider context of the Russian-Ukrainian conflict. Therefore, in line with the utilized legal framework of the Tallinn Manual, the cyber incident of the Ukrainian power grid cannot be labeled as an act of war.

**CONCLUSION**

The application of the Expert’s legal conceptualization of cyber-attacks demonstrated that neither the DDoS and defacement incidents during the Georgian-Russian back in 2008 nor the Ukrainian power grid outage in 2015 could be viewed as acts of war. In both cases, the attacks could not be directly attributed to the Kremlin, essentially disqualifying them as acts of war.

One could therefore argue that cyber-attacks, as acts of war, have not occurred yet; at least, not in accordance with the characterization proposed by the International Group of Experts, authors of the Tallinn Manual. The essence of cyber-attacks lies in the consequential harm they trigger as this mean of violence seldom entails the release of kinetic force. The harm caused by a cyber-attack manifests itself either in the damage it induces on individuals or objects as well as in the disruption – either in physical or digital terms – it begets in the functionality of targeted objects. A cyber-
attack, carried out under the overall control of a participant State, with such consequences amounts to an act of war. To unmask the latter, however, due to the technical complexity of the cyber space, is highly problematic. This arguably invokes a question that, despite lying outside the scope of the present essay, provides food for thought for further academic inquiry; will it be ever possible to classify cyber-attacks as acts of war or will the intricate nature of attribution always thwart such characterization?

**BIBLIOGRAPHY**


