International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(2): 122-129
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

The Consequences of State-Level Intrusions: A Risk Worth Taking?

Murdoch Watney
Department of Public Law
University of Johannesburg
Johannesburg, South Africa
mwatney@uj.ac.za
This article is based on research supported in part by the National Research Foundation of South Africa (UID85384). Opinions expressed are those of the author and not the NRF.

ABSTRACT

Over the years states have intruded the cyberspace of other states. Does the offending state consider the consequences it may face for the intrusion under international law and/or at international level? Is the position at present so uncertain that a state may decide that the risk is worth taking in view of the problems experienced with establishing attribution or is the injured state being second guessed on its reaction? This discussion explores, with reference to examples of state-level intrusions, whether the intrusion is prohibited under the international law or not and the possible consequences the offending state may face. The danger exists that as countries develop and/or improve their cyber capabilities, they may follow the example of countries who had intruded the cyberspace of other countries. It will be difficult for the latter to preach restraint from the moral high ground. Past state behaviour illustrates that states will put national interests and aspirations above trust, openness and transparency in cyberspace. Cyberspace is becoming a crowded place where state behaviour necessitates governance otherwise cyberspace will become lawless to the detriment of all states including those states who in the past may have decided state-intrusion is a risk worth taking.

KEYWORDS

International law, cyberspace, state-level intrusion, consequences, state accountability, attribution, state behaviour.

1 INTRODUCTION

In 2007 Israeli aircraft were able to enter the Syrian airspace undetected. This was made possible after Israel had manipulated the Syrian computerized air defense radar system into not displaying aircraft entering its airspace. As a result of this cyber manipulation, Israel successfully bombed a facility in Syria which was allegedly being built for the development of a nuclear weapon [1].

Although Syria and Israel are neigbouring countries, their relationship can be described as hostile and it is therefore not surprising that Israel saw the possible development of a nuclear weapon as a serious threat to its national security. [1] In the given example Israel sent out a clear message to Syria and other countries that it would take matters into its own hands and defend its national security interest where international obligations under the international law are ignored. It may also have paved the way for the 2010 usage of the Stuxnet worm against Iran.

The above-mentioned cyber intrusion, which can be classified as air defense radar system manipulation, should have been a wake-up call to the international community that not only do some countries have the cyber capabilities to achieve such intrusion, but it will also be used. The report that as many as 13 planes flying over Europe vanished from radar screens in June 2014 during an unprecedented series of blackouts that lasted 25 minutes, are worrying [2]. Air-traffic control centres in Austria, southern Germany, the Czech Republic and Slovakia all reported the same incident. Unsubstantiated claims were made that the air traffic control system may have been hacked. Playing devil's advocate and assuming that a

country may have been testing its cyber capabilities, it may be asked: which type of intrusion would it constitute; what consequences may such a country face; and would a country even take such a risk?

The core discussion focusses on the possible consequences a state may face for intruding into the cyberspace of another state and whether it is a risk worth taking. The discussion does not deal with state-level cyber intrusions where countries are engaged in physical combat (armed conflict, also referred to as *ius in bello*), but it deals with non-combat (peaceful) state of affairs where a state intrudes into the cyberspace of another country to achieve a specific objective.

Interestingly enough, although the topic under discussion is one that warrant attention, it has been neglected – some may say, even avoided - as it has the potential of evoking controversy since it touches on many complex inter-related issues, such as the international law, international politics and relations between states.

A clear understanding of the possible consequences a state may face for its role in state-level intrusion calls for a brief discussion of whether state-level intrusion is prohibited under international law, and if not, whether a state may face consequences at international level.

2 AN OUTLINE OF THE INTERNATIONAL LAW GOVERNING STATE-LEVEL INTRUSIONS

2.1 Introduction

A clear distinction must be drawn between state-on-state cyber intrusions at national and international level:

- At national level states are sovereign and may implement their own national laws which are applicable within their territory. State-level intrusion may constitute a crime within the ambit of the victim country's national laws, but as the intrusion constitutes a state-on-state intrusion, it will have to be dealt with at international level.
- At international level it will be determined whether the intrusion is prohibited in terms of the international law or not. The consequences a state may face for its role in the intrusion will depend on whether the intrusion constitutes a prohibited intrusion under international law.

2.2 Prohibited state-level cyber intrusions under international law

The following state-on-state cyber intrusions are prohibited under the international law:

1. An intervention is prohibited. [3] It is not expressly set out in the United Nations Charter, but the prohibition of intervention is implicit in the principle of the sovereign equality of states laid out in article 2(1) of the United Nations Charter.
2. The threat of or the use of force is prohibited. [3] Article 2(4) of the United Nations Charter provides that "All Members of the United Nations shall refrain in their international relations from the threat of use of force against the territorial integrity or political independence of any state or in any other manner inconsistent with the purposes of the United Nations." The prohibition is also a norm of customary international law.
3. Use of force that constitute an armed attack is prohibited [3]. Article 51 of the United Nations Charter provides that "nothing in the present Charter shall impair the inherent right of individual or collective self–defence if an armed attack occurs against a member of the United Nations until the security council has taken the measures necessary to maintain international peace and security." The article reflect the customary right to self-defence.

2.3 A void under existing international law

Although the international law provides for the above-mentioned prohibited intrusions, it does not indicate which intrusions fall within a prohibited category and/or when the threshold of a category is exceeded. International lawyers must interpret an intrusion and establish the category of intrusion and threshold of intrusion, but this is not easy and the matter is open to different interpretations.

Over the years state-level intrusions have escalated and have incorrectly been referred to as "cyber war" which is an inadequate term as it does not accurately describe intrusions between states. [4] Countries require clarity pertaining to state-level intrusions.

Against the above-mentioned background, the NATO Cooperative Cyber Defence Centre of

Excellence (CCD CoE), an international military organisation based in Tallinn, Estonia, invited an independent international group of experts (hereafter referred to as experts) in 2009 to produce a manual on the law governing cyber warfare. In 2013 the Tallinn Manual on International Law applicable to Cyber Warfare (referred to as the Tallinn Manual) was published under the directorship of Michael Schmitt, a US professor of international law [3].

2.4 Tallinn Manual as a source of international law?

There is no treaty on cyber warfare. The Tallinn Manual is not a source of international law. Schmitt as the editor of the Tallinn Manual stated: "We wrote it as an aid to legal advisers, to governments and militaries, almost a textbook. We wanted to create a product that would be useful to states to help them decide what their position is. We were not making recommendations, we did not define best practice, we did not want to get into policy" [5].

Kono [6] states that the Tallinn Manual may in future be adopted into the practice of states, but as will be illustrated hereafter, it is doubtful whether such a level of consensus regarding its application will be reached amongst all states:

- The drafting process of the Tallinn Manual has been criticized for not being representative of the international community. Mälksoo [7] observes that the experts came from American and so-called old European backgrounds. He questions the absence of experts from other countries such as China, Russia, Poland or Hungary. In defense of the Tallinn Manual it may be observed that it was not drafted under the auspices of the UN but NATO CCD CoE.
- Unfortunately some non-western countries may perceive the Tallinn Manual as a product conceptualising the law derived from the practices of western countries, especially after the unfortunate observation that the main conclusions in the Tallinn Manual are "largely congruous with those of the United States government" [7]. Some countries may feel uncomfortable with such an observation as there exists a perception – whether it is justifiable is not under discussion – that the US wishes to dominate cyberspace by enforcing its opinions and policies onto cyberspace. Edward Snowden's revelations in 2013 of US mass and unrestrained espionage practices did the US no favours as it confirmed some countries' allegations that the US is vying for state superiority in cyberspace [7].

In the light of the aforesaid, many non-western countries will most probably not support the Tallinn Manual as a so-called textbook in establishing the legal position to cyber intrusions under international law. A similar problem is experienced with the Council of Europe Convention on Cybercrime of 2001 which some countries also perceive as a European instrument. It is regrettable that the study on the application of international law to cyber intrusions was not conducted under the auspices of the UN with representation from all countries.

Be that as it may, the Tallinn Manual cannot be excluded from a discussion on state-level cyber intrusions. It is the only guide on cyber warfare and therefore a most useful and valuable guide [8]. Unfortunately the Tallinn Manual is not without shortcomings which is understandable taking into account the complexities of cyber intrusion. Some of the shortcomings will be highlighted within the context of the topic under discussion.

Whether an intrusion will constitute "use of force" (rule 11 of the Tallinn Manual) or an "armed attack" (rule 13 of the Tallinn Manual) is not easily established. Acts that injure or kill persons or cause physical damage or destroy objects are unambiguous use of force. The use of force is a prerequisite for an armed attack to exist [6]. A gap exists between use of force and armed attack, but it is not easy to determine when the threshold was exceeded and use of force escalated to an armed attack [3] [6]. The Tallinn Manual focuses on a "scale and effects" approach in determining when an intrusion amounts to the use of force. The experts offer a non-exhaustive list of eight indicative criteria a state may take into account when assessing whether the intrusion has reached the use of force threshold. An armed attack constitutes a higher threshold than use of force and would be the gravest form of use of force. The experts could not agree whether the use of force that does not cause physical damage, but an adverse

effect for example financial loss, would constitute an armed attack [3] [8].

When determining whether an intrusion falls within the ambit of the international law or not, cognizance must be taken of the legal position as outlined in the Tallinn Manual as well as the interpretations given by commentators on the international law.

3 APPLICATION OF THE INTERNATIONAL LAW TO PRACTICAL EXAMPLES OF STATE-LEVEL INTRUSIONS

Much has been written on this aspect [9]. The purpose of briefly discussing the application of the international law with reference to examples is to lay the groundwork for the discussion hereafter at paragraph 4 of the consequences a state may face for intruding into the cyberspace of another.

Example 1: Use of a cyber intrusion in combination with conventional weapons while countries are not engaged in physical combat

The Tallinn Manual is only applicable to cyber-to-cyber operations and does not address whether the cyber intrusion in the Israeli-Syrian example fall under international law. Kono [6] is of the opinion that such an operation qualify as part of an armed attack when it is an integral part of the whole attack even if it does not cause physical harm. However, it may be argued that Israel's intrusion was justifiable as anticipatory self-defence to protect its national security. It may be asked: What would the position under international law have been had Israel only disabled the traffic radar system, but then decided not to proceed with the physical attack?

Example 2: Distributed Denial of Service attacks

In 2007 Estonia decided to relocate a Soviet war memorial, namely a statue of a Russian soldier who had fought during World War II, to a military cemetery [1]. The decision of Estonia resulted in an outcry from Estonians of Russian descent and Russia which saw such removal as an affront to Russia's national interests. The consequence of Estonia's decision saw the first cyber intrusion of its kind being launched against a state's information infrastructure as a whole. The DDosS attacks targeted for example websites of the government, political parties and banks [10]. It lasted three weeks and caused a lot of inconvenience and disruption which resulted in significant economic damage since virtually all online business transactions could not be processed for several days. Any business that earned revenue through online advertisements on their websites lost income while their websites were down. Although Russia was accused of being behind the attacks, which it denies, not everyone believed the denial [10]. The experts of the Tallinn Manual are of the opinion that the intrusion never reached the threshold of use of force and therefore did not constitute an armed attack, although at the time of the intrusions many referred to it as cyber warfare [3].

Example 3: Usage of malware

Israel and the US were concerned about Iran's continued insistence on developing a nuclear weapon which these countries saw as a threat to national and global security [10]. Taking into consideration the successful 2007 Israel-Syria intrusion, these countries – (unofficially confirmed in 2012 [11]) – used the Stuxnet worm in 2010 to sabotage uranium enrichment centrifuges controlled by high-frequency converter drivers used by the uranium enrichment facility at Natatz. The malware had been injected into the network not by means of the internet, but by means of infected removal media [10].

The experts of the Tallinn Manual were divided as to whether the usage of Stuxnet constituted an armed attack, but the majority agreed that it was use of force [3]. The experts of the Tallinn Manual are of the opinion that although an armed attack and therefore cyber warfare is a distinct possibility, it has not occurred. Some commentators such as Iasiello [10] is of the opinion that it was an armed attack and the first example of cyber warfare. He substantiates his argument with reference to the sophistication of the malware, its functionality, the intent behind its deployment and its clandestine appearance on a non-internet connected industrial control system network. Interestingly enough, Fidler [12] is of the opinion that it did not reach the threshold of use of force because of state practice. The Stuxnet example clearly illustrates how

different interpretations may be given to the same intrusion.

Example 4: Espionage

State-level espionage is not new. The experts of the Tallinn Manual indicated that state-level espionage is not prohibited under international law [3]. It may be seen as interference in the sovereignty of a state, but it is not a prohibited intrusion. In 2013 Snowden, a former US National Security Agency contractor, revealed that the US had employed unrestrained espionage practices to collect mass information of various heads of state and citizens in other countries [13]. The US defended itself by indicating that the motivation for the surveillance was the protection of national security [14]. The US however, accused China of employing unrestrained industrial espionage with the purpose of stealing US trade secrets to the detriment of the US economic security [1]. Countries such as Taiwan also accused China of espionage [15].

4. CONSEQUENCES FACING A STATE FOR INTRUDING INTO THE CYBERSPACE OF ANOTHER STATE

4.1 Introduction

A state entering the cyberspace of another state faces consequences of which many are uncertain. An offending state cannot foresee or predict how the victim (injured) state will react to the intrusion within the international arena. In the light of this uncertainty, a state may decide that the risk of state-level intrusion is worth taking.

Most states will not openly acknowledge that it had intruded into the cyberspace of another. The purpose of the intrusion is to secretly, quickly and anonymously enter the cyberspace of another state to achieve a specific objective. The characteristics of cyberspace make attribution of the intrusion to a state difficult. It is possible for a state to hide the origin of its intrusion. In the absence of conclusive proof of the offending state's intrusion, it is easy for a state to deny the intrusion and escape accountability.

However, in some instances evidence confirming attribution is so conclusive that a state cannot deny the intrusion. A good example is the 2013 Snowden revelations of US unrestrained espionage practices [13]. In other instances, there may not be conclusive evidence, but there may be strong circumstantial evidence as well as suspicions linking the state to the intrusion, for example the Estonian DDoS attacks and allegations that Russia supported the patriotic hacktivists [7] [10]. However, attribution to a state is not possible without conclusive proof. Rule 7 of the Tallinn Manual [3] states that the mere fact that a cyber operation has been launched from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that state. This is exactly the claim the Russian government made (as well as China in 2001) when the US networks were intruded [1]. A country may at a later stage unofficially acknowledge the intrusion, such as the US in respect of the Stuxnet worm [11]. Countries may also deduce from international politics and relations between states which state(s) may have been responsible for the intrusion.

4.2 Legal consequences under international law

The international legal system has no central authority to enforce compliance with the international law. In these circumstances states claim the right to enforce compliance with rules of the international law by responding to an illegal act with a reciprocal illegal act designed to compel compliance [16].

If an intrusion is prohibited under international law and there is conclusive evidence confirming the intrusion attributable to a state, then the offending state may face the following possible legal consequences:

- The offending state may be held responsible under the law of state responsibility for its wrongful act. Dugard [16] indicates that where a state commits an international wrong against another state, it incurs international responsibility. In such a case an offending state is obliged to make reparation.

The experts of the Tallinn Manual [3] indicated that the injured state may only use countermeasures to induce compliance with international law by the offending state. The majority of experts agreed that if the international wrongful act in question has ceased, the victim state is not entitled to initiate or

to persist in countermeasures [3]. Cyber countermeasures may not involve a threat of or use of force (rule 11 of the Tallinn Manual). The experts also distinguished between countermeasures and acts of retorsion. Acts of retorsion are so-called unfriendly, although lawful measures, a state takes against another, for example during the 2007 Estonian cyber intrusions, Estonia suspended some services to Internet Protocol (IP) addresses from Russia [3]. Other examples of retorsion are limitation of normal diplomatic relations, a trade embargo not in violation of a treaty obligation or termination of an aid programme [16].

- Where the offending state was responsible for an armed attack, the victim state may resort to use of force under article 51 of the UN Charter. A victim state may only act in self-defence if it was the victim of the most grave form of use of force constituting an armed attack [6]. The victim state does not have an unlimited right to use force and it must adhere to the conditions of necessity or proportionality based on customary international law. Kono [6] indicates that the issue of anticipatory self-defence against a cyber attack will have to be discussed in future. At present the Tallinn Manual allows a victim state to take anticipatory actions even before an armed attack has been launched [3].

Taking into consideration that determining the category of intrusion and/or establishing conclusive proof of attribution may be stumbling blocks to state accountability, the offending state may decide that the risk is worth taking.

4.3 Consequences at international level

A state may not incur consequences under the international law, either because the intrusion is not prohibited, such as espionage or the injured (victim) state may have decided not to take action, either because of the challenges relating to establishing accountability or because the injured state does not want to damage its relations with the offending state.

At international level the offending state runs the risk of not achieving the objective with the intrusion and at the same time damaging its international relations with the injured state and other states that may have come out in support of the victim country. Russia may have thought that Estonia would give in to its demand not to remove the statue, but Estonia did not change its decision [10]. Estonia publicly acknowledged it had been the victim of a massive cyber intrusion and it accused Russia of orchestrating the attacks which Russia denied. Many NATO countries came out in support of Estonia and interestingly enough, the attacks firmly placed Estonia on the world map. NATO took the attacks so seriously that in 2008 the CCD CoE was established in Estonia. The attacks may have had a positive spin-off for Estonia, but Iasiello [10] indicates that if the state behind the attacks was indeed Russia as circumstantial evidence suggests, then it was an unqualified failure as an instrument of public policy as it was unsuccessful in enforcing the Russian policy onto another country.

Stuxnet clearly illustrates that the intrusion may not have been worth the risk. Although the Stuxnet worm delayed the development of a nuclear bomb, it is now doubtful whether it delayed the development permanently. Stuxnet was unfortunately not contained at the Natanz nuclear energy facility, but it spread beyond Iran and may be used against other countries [1]. Although Iran may not have publicly accused the US for the state-level intrusion, it employed state-level intrusions in retaliation. In 2012 Iran attacked Amcu, a Saudi-Arabian oil plant and left behind a “calling card” of a burning US flag. [10] Iran then went on to launch a series of sequential attacks against the US financial industry including JPMorgan and Wells Fargo which resulted in the slowing down of overwhelmed servers and denying customers access to the bank services [10] [15]. Iran may have acted in retaliation to indicate to the US that it does have the cyber capabilities to intrude into the US cyberspace and that it will not accept intrusions into its cyberspace.

Other countries may not have voiced their reservations of the usage of Stuxnet, but the use of what may be referred to as a cyber weapon has created a militarized environment where such intrusions may be seen as acceptable. Knake, [1] a former US security advisor, indicated that the US had crossed a rubicon and that the reversal of the consequences that came with the Stuxnet usage might not easily be accomplished. He warned that “the US has also launched what is likely to be a

cyber boomerang, a weapon that will someday be used to attack some of America's own defenseless networks." [1]

The 2013 Snowden espionage revelations illustrate how a country may be seen as a so-called rogue country within the international community. [17] Countries are suspicious of the US motives for spying on them. The US has indicated that it gathered information for national security purposes, but some countries see the intrusions as enforcing its superiority onto cyberspace and advancing only its own national interest to the detriment of the existence of trust, openness and transparency in cyberspace. [17] Practicing restraint would have given the US a leg to stand on when complaining about other countries' state-level intrusions and also in respect of cyberspace governance.

4.4 Legal consequences at national level of a state

Addressing state-level espionage at international level by means of diplomatic discussions may not be successful. The US has on numerous occasions accused China of industrial espionage which allegations China has vehemently denied. [1]

In May 2014 the US took an unprecedented step and one that may have taken China and other countries by surprise when it instituted criminal charges against 5 Chinese military personnel who had allegedly committed industrial espionage on behalf of the Chinese government by gathering US trade secrets. The US decision to institute criminal charges against Chinese nationals conveyed a symbolical message to the offending state, China, that it would not tolerate such state-level intrusions [18]. The US must have weighed the Chinese-US espionage practices against a subsequent strained US-China relationship and must have decided that US economic security outweigh smooth international relations. Only time will tell if such state actions will have the desired effect on the offending state.

5 CONCLUSION

Although cyberspace allows for state-on-state intrusions, it does not imply a state should intrude into another state's cyberspace merely because it is able to. As illustrated, in some instances the offending state did not achieve the objective for the intrusion. A state may feel the risk outweighs the consequences it may face, especially as it is not clear which consequences a state may face. In the light of past intrusions, states may have a perception that state-level intrusions are acceptable and that anything goes in cyberspace. It is time that acceptable state behaviour is established under the international law otherwise cyberspace may become a place where states willy-nilly pry on other states to advance their own interests and power or retaliate against the intrusion. Clarke [1] is correct when he states: "…if you are going to throw cyber rocks, you had better be sure that the house you live in has less glass than the other guy's, or that yours has bulletproof windows." But do states wish to inhabit such a world? I would hope not.

6 REFERENCES

1. Clarke, R.A, Knake, R.K.: Cyber War. HarperCollins Publishers, New York (2012).
2. Day, M.: "13 Planes vanish from radars over Europe," http://www.telegraph.co.uk/news/worldnews/Europe/Austria/10898385/13-planes-vani...
3. Schmitt, M.N.: Tallinn Manual on the International Law applicable to Cyber Warfare, New York, Cambridge University Press (2013).
4. Smith, P.: "How seriously should the threat of cyber warfare be taken?" http://www.e-ir.info/2014/01/17how-seriously-should-the-threat-of-cyber-warfare-be..
5. Zetter, K.: "Legal experts: Stuxnet attack on Iran was illegal act of force," http://www.wired.com/threatlevel/2013/03/stuxnet-act-for...
6. Kono, K.: "Briefing Memo: Cyber Security and the Tallinn Manual", www.nids.go.jp/english/pubicatoon/pdf/.../briefing_e180.pdf
7. Mälksoo, L.: "The Tallinn Manual as an international event." http://www.diplomaatia.ee/en/article/the-tallinn-manual-as-an-international-event/
8. Vihul, L.: "The Tallinn Manual on the International Law applicable to cyber Warfare", http://www.ejiltalk.org/the-tallinn-manual-on-the-internation...
9. Watney, M.M.: Challenges pertaining to cyber war under the International Law. In: The Third international conference on Cyber Security, Cyber Warfare and Digital Forensics pp. 1- 5 (2014).
10. Iasiello, E.: "Cyber Attack: A Dull Tool to Shape Foreign Policy," http://www.ccdcoe.org/publicatoins/2013/proceedings/d3r1s3_Iasiello.pdf

11. Leyden, J.: "Cyberwarfare playbook says Stuxnet may have been 'armed' attack", http://www.theregister.co.uk/2013/03/27/stuxnet_cyver war_r...
12. Fidler, D.P.: "Was Stuxnet an Act of War? Decoding a Cyberattack", http://ieeeexplore.ieee.org
13. Leigh, D. Harding, L.: Wikleaks. Guardian Books, UK (2013).
14. Lucas, E.: "Edward Snowden: Did the American whistleblower act alone?" http://www.telegraph.co.uk/news/worldnews/northame rica/usa/10595021/Edward-Sn
15. France-Presse, A.: "Taiwan sets up internet shield to tackle 'hacking," http://www.scmp.com/news/china/article/1195632/taiw an-set...
16. Dugard, J.: International Law: A South African Perspective. Juta, Cape Town, South Africa (2011).
17. Matthew, J.: "Edward Snowden NSA Scandal: China calls on international community to form cyberspace code of conduct." http://www.ibtimes.co.uk/edward-snowden-nsa-scandal-china-merkel-obama-517736
18. Beauchamp, Z.: "How the US indictment of Chinese military hackers will change cyberespionage." http://www.vox.com/2014/5/19/5731696/chinese-hackers-cyberespionage-theft-cyber...