RESEARCH ANALYSIS
DECEMBER 2017

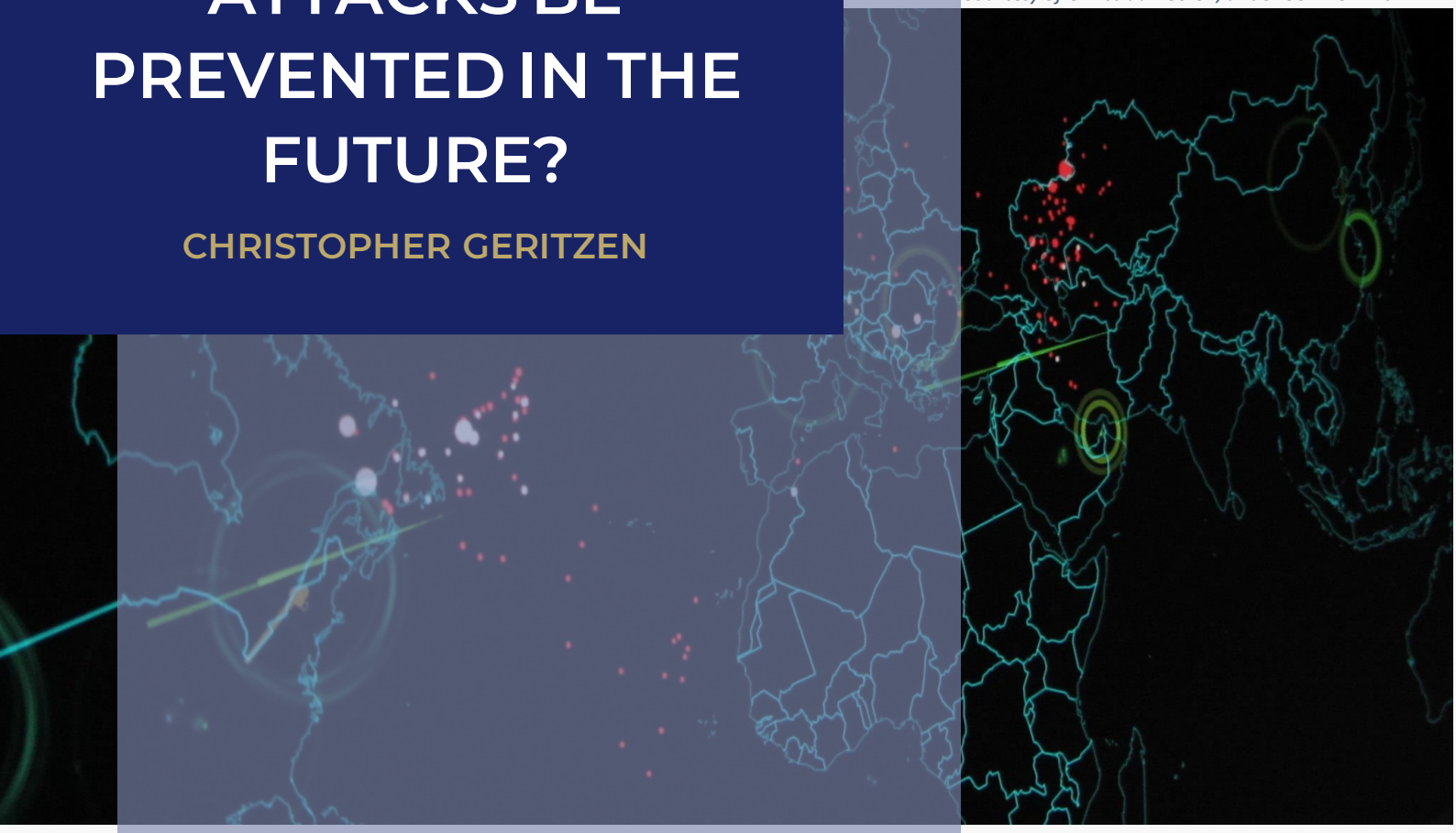
THE INTERNET OF THINGS: A WEAPON OF MASS DISRUPTION?

-

THE CASE OF THE MIRAI MALWARE: CAN SIMILAR DDoS ATTACKS BE PREVENTED IN THE FUTURE?

CHRISTOPHER GERITZEN

UNIVERSITÀ DEGLI STUDI FIRENZE



Center for Cyber Security and International Relations Studies

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Le dichiarazioni e le opinioni espresse nella presente relazione sono unicamente quelle dell'autore e non implicano l'approvazione da parte dell'Università di Firenze, del Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali o del Center for Cyber Security and International Relations Studies.

Center for Cyber Security and International Relations Studies

THE INTERNET OF THINGS: A WEAPON OF MASS DISRUPTION?

-

THE CASE OF THE MIRAI MALWARE: CAN SIMILAR DDoS ATTACKS BE PREVENTED IN THE FUTURE?

Christopher Geritzen

UNIVERSITÀ DEGLI STUDI FIRENZE

Research Analysis

December 2017

THE INTERNET OF THINGS: A WEAPON OF MASS DISRUPTION?
-
THE CASE OF THE MIRAI MALWARE: CAN SIMILAR DDoS ATTACKS BE PREVENTED IN THE FUTURE?

1 Introduction

Distributed Denial of Service (DDoS) have been used with political motivations on different occasions, a prominent example being the cyberattack on Estonia in 2007 which was neither the first nor the last case (Nazario, 2009). In 2009, President Barrack Obama referred to, among other things, botnets – the tool that is used to conduct DDoS attacks – as "weapons of mass disruption" (cited in Sanger & Markoff, 2009). This paper will investigate whether the Internet of Things (IoT) is a "weapon of mass disruption". In order to answer this question, it will take a look at IoT-based DDoS attacks and whether there are ways to prevent similar attacks in the future. It will show that IoT-based attacks are much more capable than previous, "regular" DDoS attacks. However, before doing so, it will first show the relevance of this topic for International Relations (IR) by looking at the political and international aspects of DDoS attacks as well as their potential impact on the international system and their use for political reasons.

2 Distributed Denial of Service Attacks and International Relations

2.1 Introduction to Distributed Denial of Service Attacks

"DDoS attacks are among the most visible and disruptive of cyber-attacks" (Nazario, 2009:p.2). This section will explain the basic idea behind DDoS attacks but will not go into all technical details as this would be outside the scope of this paper. However, additional aspects of DDoS attacks will be explained at later points. A DDoS attack is a form of cyberattack that aims at "making an online service unavailable by overwhelming it with traffic from multiple sources" (Anon, n.d.). Those attacks are usually conducted using botnets, which are networks of

compromised devices that are "controlled remotely, without [the device] owners' knowledge" (Anon, n.d.). A very simple form of a DDoS attack would be a number of people "continuously reload[ing] a website" (Nazario, 2009:p.1) thereby overwhelming it.

In general, "cyber weapons are [...] complicated, expensive, and difficult to utilize for offensive and defense intent" (Valeriano & Maness, 2017:pp.260–261). However, this is not the case for DDoS attacks, which "provide a simple, easily available mechanism to disrupt the Internet presence of a group or a small nation" (Nazario, 2009:p.18) and are in addition to that rather cheap since "[a] weeklong DDoS attack, capable of taking a small organization offline can cost as little as $150" (Anon, n.d.).

2.2 The Relevance of Distributed Denial of Service Attacks for International Relations

The relevance of DDoS attacks for IR can be structured along three different aspects. First, current state of affairs when it comes to cyberattacks and in particular DDoS attacks. Second, the potential future impact of cyberweapons in general on the international system. Third, the use of DDoS attacks as a means of censorship. Each of the three aspects will be addressed in this section.

In order to describe the current state of affairs, the cyberattack on Estonia in 2007 (in the following called the 'Estonia case') will be used for different reasons. To start off, it is among the most studied cyberattacks with a political dimension in the literature, even though many more examples exist (Nazario, 2009; Kozlowski, 2014; van der Meer, 2015). Moreover, it consisted out of DDoS attacks aimed at "websites of ministries, banks, media, and political parties" (van der Meer, 2015:p.2), and most importantly, it shows very well the various international dimensions of DDoS attacks. Those international dimensions can be divided into two layers. The first layer consists of the technical aspects and serves as the foundation for the second layer which contains the political aspects. Two key technical aspects can be identified which will be explained in the following together with the political aspects arising from each.

1. The first technical aspect is that the attack came not from one specific point of origin but was "widely distributed [and] sourced [...] from all over the world" (Nazario, 2009:p.12). Related to that,

the majority of "cyber-attacks originate from abroad" (van der Meer, 2015:p.1).

Considering this aspect, we can see that the attack itself is internationalised in two ways. The first aspect is closely related to the nature of DDoS attacks and makes interstate cooperation necessary to mitigate them. In the Estonia case, this took place "through the network of cyber experts" (van der Meer, 2015:p.7) while in another case, a DDoS attack against US banks in 2012, diplomatic channels were successfully used to request the removal of malware from servers in different countries, which mitigated the attack (van der Meer, 2015).

The second aspect makes international cooperation necessary when it comes to prosecuting the perpetrator. While "many potential uses of cyberweapons constitute crimes in most jurisdictions" (Stevens, 2017:p.26) most perpetrators are located in other states. This was also the case in the Estonia case where perpetrators where identified to be located in Russia (van der Meer, 2015) Thus, cooperation between Estonian and Russian authorities would have been necessary but did not happen for reasons that will be addressed in the context of the next aspect.

2. The second technical aspect is that it is not possible to "attribute any of these attacks to a specific group or agency" (Nazario, 2009:p.12). This is known as the "attribution problem" and is a common issue when it comes to identifying the perpetrator behind a cyberattack (Nazario, 2009; Farrell, 2014). However, the "attribution problem" does not prevent "politicians [...] from quickly blaming a specific adversary" (Goth, 2007:p.2).

The "attribution problem" can also be seen in the Estonian case. Estonia publicly accused Russia of being the perpetrator behind the attacks as they took place in the context of "[tense] diplomatic relations between Estonia and Russia" (van der Meer, 2015:p.2) due to "the relocation of a Sovietera war memorial in Tallinn" (van der Meer, 2015:p.2) and were allegedly, according to the Estonian Minister of Foreign Affairs, connected to the Russian government (van der Meer, 2015). While there are arguments that support this claim and the "attacks would have fit into Russia's overall foreign policy strategy" (Schmidt, 2013:p.21) it is not possible to actually prove the involvement of the Russian government (Schmidt, 2013). Furthermore, the "public accusation did not have any positive effects" (van der Meer, 2015:p.7) In fact, the public accusation

might even be the reason for the lack of cooperation when it came to prosecuting the identified perpetrators in Russia (van der Meer, 2015). Coming back to the "attribution problem", it is necessary to state that it provides states that make use of such attacks with plausible deniability as it allows them to use them in support of their policy without being directly connected to it for "modern information warfare" (Nazario, 2009:p.12). In other words, states cannot be held accountable for their actions as the actions cannot be attributed to them.

In summary, the above illustrates the physical separation between the tool that is used for the attack, the botnet that is distributed all over the world, the perpetrator, who is located in one country, and the target which is located in a different country, as well as the problems this can bring for mitigating the attack and prosecuting the perpetrator.

Finally, the Estonia case made it clear that – independent from who the perpetrator was and whether there has been state involvement – "cyber attacks can be used as a tool in international or bilateral conflicts" (Schmidt, 2013:p.22). Going even further than that, it was widely referred to as "the first cyberwar in history" (Kozlowski, 2014:p.239). Schmidt (2013), while acknowledging the importance of the attack, disagrees with this sentiment, stating that it "was not a war when one applies a serious and sober definition of that term" (Schmidt, 2013:p.22). Furthermore, Estonia was neither the last nor the first example for a DDoS attack with a political dimension (Nazario, 2009:p.3).

Now that the current state of affairs has been addressed it makes sense to look at the potential future impact of cyberattacks on the international system. Here, Rustici (2011) outlines an interesting scenario in which "cyberweapons [...] become an equalizing force" (Rustici, 2011:p.33) because they "are a cheap way to build a global strike capability against networked states" (Rustici, 2011:p.37). In other words, less powerful states would be able to use cyberweapons with great effect against classically powerful states. Thus, cyberweapons would act as a form of deterrence against "interventionist foreign policies [which] would become exceedingly costly" (Rustici, 2011:p.37). This would possibly lead to a decrease of violence on the one hand but would, on the other hand, also "make the world a safer place for corrupt and abusive regimes" (Rustici, 2011:p.38) as for example humanitarian interventions would come at a much higher potential cost.

The third point that needs to be considered regarding cyberattacks and here in particular DDoS attacks, is their potential to be used as a means of censorship. Due to their previously described characteristics, their ability of disrupting services, and the importance of the internet as "major communication tool for news media, governments, political parties, the opposition and dissidents" (Nazario, 2009:p.12), DDoS attacks are a useful "tool of censorship" (Nazario, 2009:p.18) This is supported by Krebs (2016d)who explains that the defence against DDoS attacks by using specialised services is with a cost of between $150000 and $200000 simply too expensive for, for example, independent journalists. He calls this development the "Democratization of Censorship" (Krebs, 2016d), which is a fitting term considering the cost of defence and the easy availability of DDoS attacks to both state and nonstate actors alike.

3 Distributed Denial of Service Attacks and the Internet of Things

3.1 The Connection Between Distributed Denial of Service Attacks and the Internet of Things

The previous part of this paper has explained the problem of DDoS attacks and their relevance to IR. This part will go on to explain the connection between the IoT and DDoS attacks. It will show that the IoT has the potential to be turned into a "weapon of mass disruption" that is far more capable than past DDoS attacks, such as the one on Estonia in 2007, which did not cause much damage (Schmidt, 2013; Kozlowski, 2014). The "'Internet of Things' will lead to an exponential of number of devices being connected to the network" (Ebert & Maurer, 2017) Those networked devices – the list includes household appliances, smart home devices, internet cameras, and routers – are not known for their security and in fact have many vulnerabilities (Barcena & Wueest, 2015). Due to their "large volume, pervasiveness, and high vulnerability [they] have attracted" (Kolias et al., 2017:p.80) the attention of people conducting DDoS attacks as IoT devices are in addition also always online (Kolias et al., 2017).

Furthermore, Kolias et al. (2017) have identified five reasons that make "IoT devices [...] particularly advantageous for creating botnets":

1. They are always online.
2. They lack security.

3. They are operated "under [a] setup-and-forget" (Kolias et al., 2017:p.83) mindset and not properly maintained.
4. They can provide "[c]onsiderable attack traffic" (Kolias et al., 2017:p.83).
5. They "require minimum user intervention" (Kolias et al., 2017:p.83) and the end-user cannot easily "fix" a compromised device.

The above has shown the potential of IoT devices to be abused for DDoS attacks. In the next section it will be shown that this is not a science fiction scenario but has already happened in reality.

3.2 The Mirai Malware

Mirai is a malware that "spreads to vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default usernames and passwords" (Krebs, 2016e). It compromises IoT devices which are then combined into a botnet that can be used for DDoS attacks (Krebs, 2016e; Kolias et al., 2017). While it is not the only example for a malware that builds IoT-based botnets it is a very prominent one which was used in multiple attacks (Kolias et al., 2017) It is important to note that malware with a similar purpose, sometimes but not always based on Mirai, continues to proliferate (Kolias et al., 2017). The following sections will take a look at two attacks in particular 6 that demonstrate the power of an IoT-based DDoS attack and show the potential of the IoT as a "weapon of mass disruption".

3.2.1 The Attack on the KrebsOnSecurity Blog (September 2016)

The first case is the attack on the cyber security blog of Brian Krebs, which was "twice the size of the next-largest attack [his protection provider Akamai] had ever seen before" (Krebs, 2016d) and eventually forced his website to go offline as Akamai was unable to keep up the free protection they had provided without "[causing] problems for the company's paying customers" (Krebs, 2016d). The attack stood out because of its unprecedented size but also because it did not make use of common ways that are used to increase the capacity of DDoS attacks like the next-largest attack did but only used the traffic provided by the compromised devices (Krebs, 2016c). This shows that the potential of IoT-based DDoS attacks is far beyond "regular" DDoS attacks.

3.2.2 The Attack on Dyn (October 2016)

The second case is the attack on the Domain Name System (DNS) provider Dyn, which caused "outages and slowness" (Krebs, 2016a) for services and websites such as, among many others, "Twitter, Netflix, Spotify" (Perlroth, 2016). DNS can be likened to a "phone book for the internet" (Gonyea, n.d.) and translates "human-readable hostnames like www.dyn.com into machine-readable IP addresses" (Gonyea, n.d.). In the absence of the DNS, websites can only be reached directly via entering their IP address (Gonyea, n.d.). This means that "while the attack did not affect the websites themselves, it blocked or slowed users trying to gain access to those sites" (Perlroth, 2016). The attack lasted for "nearly 12 hours [and was] the largest and strongest DDoS attack known to date" (Anon, 2016a). Furthermore, the attack caused considerable losses to the affected services as they were temporarily unavailable (LaFrance, 2016).

4 Prevention of Similar Attacks: Is it Possible in Theory and Can it be Realised?

4.1 Addressing the Source of The Problem?

Considering the attack vector that was used by the Mirai malware, the problem results from a lack of security (Anon, 2016b; Krebs, 2016a; Kolias et al., 2017). In particular, Mirai relied on a list of publicly available default passwords in order to compromise the IoT devices (Krebs, 2016e). Some of those passwords were even hard-coded into the device and in some cases the password for the device's remote access – the entry point of Mirai – did not change even when the user changed the device password (Krebs, 2016e, 2016c). For this particular method of compromising devices, a replacement of default password with mandatory user set passwords would be a solution (Dormann cited in Krebs, 2016e). In fact, "several IoT device makers [...] have begun to require unique passwords by default" (Krebs, 2016e). However, this does not solve the general security problem that is a result of "IoT device vendors' chronic neglect in applying even basic security practices" (Kolias et al., 2017:p.81). A general solution "might be government action, in the form of required security standards" (Anon, 2016b). Kolias et al. (2017) agree that, "enforce[ing] [...] robust security standards" (Kolias et al., 2017:p.84) is necessary. Recently, both in the US and Europe there have been actions going into that direction in order to, for

example, require security updates and prohibit default passwords (Krebs, 2016b, 2017). The outcome of those proposals remains to be seen. However, even a year after Mirai's first sighting the same attack vector is still exploited (Kolias et al., 2017).

Furthermore, government regulation takes some time until it shows result. It would not immediately affect existing vulnerable or compromised devices. To solve the problem of those devices, different solutions have been proposed that make use of something that is similar to Mirai but instead of compromising the devices for use in a botnet, it would work to secure the device. Examples for those solutions can be found in Cao et al. (2017) and De Donno et al. (2017). Discussing those options in detail would unfortunately go beyond the scope of this paper. However, one should note that both come with their own limitations (Cao et al., 2017; De Donno et al., 2017). For example, De Donno et al. (2017) see a significant potential for abuse when it comes to their own proposal and state that "[they] feel that the path traced by AntibIoTic should not be taken by anyone, because it could unexpectedly backfire" (De Donno et al., 2017:p.10) but further state that the situation is bad enough to consider such measures (De Donno et al., 2017). Cao et al. (2017) also see different issues with their approach but also state that their system is secure as well as – based on their experiments – "both simple and effective" (Cao et al., 2017:p.14). It "provides an attractive path towards mitigating the threats from Mirai, until all the vulnerable devices are retired" (Cao et al., 2017:p.14). It thus might be a viable short-term solution until the long-term solution of government regulation is implemented. However, it remains to be seen in how far it will be effective outside of experiments.

4.2 An International Regime Regulating Cyberweapons?

A solution that addresses the use of cyberattacks, including DDoS attacks, by states might be an international regime that regulates the use of cyberweapons. However, such a regime does so far neither exist nor is its emerging "imminent" (Stevens, 2017:p.4). Stevens (2017) has identified four reasons for the absence of such a regime:

1. NATO member states "[construct] cyberweapons as legitimate military instruments" (Stevens, 2017:p.6) that are therefore governed by the same international regimes as other weapons. They do not see the need for a separate regime as one is already in place.

2. The United States are "the dominant producer and consumer of cyberweapons components" (Stevens, 2017:p.16).
3. "Cyberweapons governance is hampered by the nature of the digital environment" (Stevens, 2017:p.24). In other words, the structure of the Internet works against governance.
4. The "great powers – US, Russia, China – prevent policy coordination and the formation of a global regulatory regime or prohibition regime for cyberweapons" (Stevens, 2017:p.20) as a result of their vastly different stances and opinions when it comes to cyberweapons.

Another reason that ties into the third point is that "monitor[ing] states' cybersecurity activities" (Farrell, 2014) is almost impossible which makes it different from "troops movements [...] or nuclear facilities" (Farrell, 2014) that are much easier to monitor. This together with the previously described "attribution problem" makes it hard to identify non-compliance with any potential regime (Farrell, 2014). In summary, an international regime regulating cyberweapons is both unlikely to emerge and unlikely to be actually effective.

5 Conclusion

With the findings of the previous sections in mind we come back to the initial question whether the IoT is a "weapon of mass disruption". Considering the nature and security problems of the IoT together with their active exploitation by Mirai and other malwares the answer this paper has found is that the IoT currently is being used as a "weapon of mass disruption" as the examples of attacks with Mirai-based botnets show. However, it also has been shown that this is not inevitable as there are ways to prevent or mitigate the proliferation of Mirai and Mirai-based malwares on the one hand and ways to prevent something similar from happening again in the future on the other. However, the effectiveness of both the short- and the long-term solutions remains to be seen and further research into the possibility of government regulation as a long-term solution is necessary. Furthermore, considering the usefulness of DDoS attacks as a cyberweapon for state actors, the "willingness of capable states to use offensive cyber capabilities" (Stevens, 2017:p.25), and the reasons for the nonexistence of an international regime regulating cyberweapons, it would make sense to investigate in how far all states are actually interested in an

effective long-term solution. Fortunately, device manufacturers could remove or mitigate the issue, even if state regulation does not happen or is unsuccessful, through better device security, which some have started to implement (Krebs, 2016e). Additionally, at least some security researchers working on short-term solutions to the problem are willing to work with device manufacturers (Cao et al., 2017). In conclusion, while the IoT currently is being abused as a "weapon of mass disruption" there are ways to prevent this from happening in the future that should be investigated in more detail.

In summary, the described attacks, which are two out of many as can be seen in Kolias et al. (2017), serve as example for the potential of the IoT to be used as a "weapon of mass disruption" against individual websites or even Internet infrastructure. The following section will consider whether there are realistic possibilities to prevent this from happening again and again in the future.

6 Acknowledgement

This paper was originally written for the Student Conference "Peace for Security or Security for Peace" on 19 and 20 January 2018 at the Hochschule Rhein-Waal (HSRW, Rhine-Waal University of Applied Science) in Kleve, Germany. The author would like to thank **Dr. Jan Niklas Rolf** for the helpful comments and for encouraging the submission of this paper to the Center for Cyber Security and International Relations Studies.

7 References

Anon (2016a) *October 2016: Black Five Client Advisory, Dyn / DDoS Attack.* [Online]. Available from: http://www.red5security.com/news_media_34_3921121624.pdf [Accessed: 12 October 2017].

Anon (2016b) The internet of stings. *The Economist*. [Online]. Available from: https://www.economist.com/news/science-and-technology/21708220-electronic-tsunamicrashes-down-solitary-journalist-internet [Accessed: 26 December 2017].

Anon (n.d.) *What is a DDosS Attack?* [Online]. Digital Attack Map. Available from: https://www.digitalattackmap.com/understanding-ddos/ [Accessed: 10 December 2017].

Barcena, M.B. & Wueest, C. (2015) Insecurity in the Internet of Things. *Security Response, Symantec.* [Online] Available from: https://www.symantec.com/content/en/us/enterprise/iot/b-insecurity-in-the-internet-ofthings_21349619.pdf [Accessed: 10 December 2017].

Cao, C., Guan, L., Liu, P., Gao, N., et al. (2017) Hey, you, keep away from my device: remotely implanting a virus expeller to defeat Mirai on IoT devices. *arXiv preprint arXiv:1706.05779*.

De Donno, M., Dragoni, N., Giaretta, A. & Mazzara, M. (2017) AntibIoTic: Protecting IoT Devices Against DDoS Attacks. *arXiv preprint arXiv:1708.05050.*

Ebert, H. & Maurer, T. (2017) *The impact of cybersecurity on international relations.* [Online]. 12 February 2017. OUPblog. Available from: https://blog.oup.com/2017/02/impact-cybersecurity-international-relations/ [Accessed: 10 December 2017].

Farrell, H. (2014) The political science of cybersecurity III – How international relations theory shapes U.S. cybersecurity doctrine. *Washington Post.* [Online] 20 February. Available from: https://www.washingtonpost.com/news/monkey-cage/wp/2014/02/20/the-political-scienceof-cybersecurity-iii-how-international-relations-theory-shapes-u-s-cybersecurity-doctrine/ [Accessed: 10 December 2017].

Gonyea, C. (n.d.) *What is Domain Name Service (DNS)?* [Online]. Available from: https://dyn.com/blog/dns-why-its-important-how-it-works/ [Accessed: 10 December 2017].

Goth, G. (2007) The politics of DDoS attacks. *IEEE Distributed Systems Online.* 8 (8).

Kolias, C., Kambourakis, G., Stavrou, A. & Voas, J. (2017) DDoS in the IoT: Mirai and other botnets. *Computer*. 50 (7), 80–84.

Kozlowski, A. (2014) Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, ESJ. 10 (7).

Krebs, B. (2016a) *DDoS on Dyn Impacts Twitter, Spotify, Reddit — Krebs on Security.* [Online]. Available from:

https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotifyreddit/ [Accessed: 10 December 2017].

Krebs, B. (2016b) *Europe to Push New Security Rules Amid IoT Mess — Krebs on Security*. [Online]. Available from: https://krebsonsecurity.com/2016/10/europe-to-push-new-securityrules-amid-iot-mess/ [Accessed: 27 December 2017].

Krebs, B. (2016c) *KrebsOnSecurity Hit With Record DDoS — Krebs on Security*. [Online]. Available from: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ [Accessed: 26 December 2017].

Krebs, B. (2017) *New Bill Seeks Basic IoT Security Standards — Krebs on Security.* [Online]. Available from: https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-securitystandards/ [Accessed: 27 December 2017].

Krebs, B. (2016d) *The Democratization of Censorship — Krebs on Security.* [Online]. Available from: https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/ [Accessed: 10 December 2017].

Krebs, B. (2016e) *Who Makes the IoT Things Under Attack? — Krebs on Security.* [Online]. Available from: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-underattack/ [Accessed: 10 December 2017].

LaFrance, A. (2016) How Much Will Today's Internet Outage Cost? *The Atlantic.* [Online]. Available from: https://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/ [Accessed: 26 December 2017].

van der Meer, S. (2015) *Foreign Policy Responses to International Cyber-attacks: Some Lessons Learned.* [Online]. Available from: https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf [Accessed: 10 December 2017].

Nazario, J. (2009) Politically motivated denial of service attacks. *The Virtual Battlefield: Perspectives on Cyber Warfare*. 163–181.

Perlroth, N. (2016) Hackers Used New Weapons to Disrupt Major Websites Across U.S. *The New York Times*. [Online] 21 October. Available from:https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html [Accessed: 10 December 2017].

Rustici, R.M. (2011) Cyberweapons: Leveling the international playing field. *Parameters*. 41 (3), 32–42.

Sanger, D.E. & Markoff, J. (2009) Obama Announces Strategy Against Cyberattacks. *The New York Times*. [Online] 29 May. Available from: https://www.nytimes.com/2009/05/30/us/politics/30cyber.html [Accessed: 10 December 2017].

Schmidt, A. (2013) The Estonian Cyberattacks. In: Jason Healey (ed.). *A fierce domain: conflict in cyberspace*, 1986 to 2012. Vienna, VA, Cyber Conflict Studies Association. p.

Stevens, T. (2017) Cyberweapons: power and the governance of the invisible. *International Politics*. [Online] Available from: doi:10.1057/s41311-017-0088-y [Accessed: 10 December 2017].

Valeriano, B. & Maness, R.C. (2017) *International Relations Theory and Cyber Security.* [Online]. Available from: http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/international_political_theory_and_cyber_security_oxford_handbook_valeriano_and_maness_2018.pdf [Accessed: 10 December 2017].

CENTER FOR CYBER SECURITY AND INTERNATIONAL RELATIONS STUDIES (CCSIRS)

Centro Interdipartimentale di Studi Strategici,
Internazionali e Imprenditoriali (CCSSII)
Università degli Studi di Firenze
Via delle Pandette 2, 50127, Firenze

https://www.cssii.unifi.it/ls-6-cyber-security.html

Center for Cyber Security and
International Relations Studies