3rd International Conference

on Public Policy (ICPP3)

June 28-30, 2017 – Singapore

Panel T09P11 Session 1

The Governance of Innovative Technologies

Title of the paper

THE ROLE OF TRANSNATIONAL EXPERT ASSOCIATIONS IN GOVERNING THE CYBERSECURITY RISKS OF THE INTERNET OF THINGS

Author(s)

Brass Irina (University College London) - i.brass@ucl.ac.uk
Sowell Jesse (Stanford University) - jsowell@stanford.edu
Madeline Carr (Cardiff University) - carrm@cardiff.ac.uk
Blackstock Jason (University College London) - jason.blackstock@ucl.ac.uk

Date of presentation

Thursday, June 29th 10:30 to 12:30

THE ROLE OF TRANSNATIONAL EXPERT ASSOCIATIONS IN GOVERNING THE CYBERSECURITY RISKS OF THE INTERNET OF THINGS

Irina Brass, Jesse Sowell, Madeline Carr and Jason Blackstock

This document is a draft. Please do not cite at this stage.

Abstract

The benefits and challenges of the Internet of Things (IoT) are increasingly capturing the attention of policy-makers, the media and the wider public. On the one hand, IoT has the potential to enable new models of organising social and economic activity, as evidenced in sectors such as transport (mobility as service) and manufacturing (industrial IoT). On the other hand, IoT is challenged by the increasing number of cyberattacks originating from unsecure connected devices and the challenges of monitoring and enforcing basic security policies on them. This paper analyses the unique cybersecurity risks emerging from the growth of IoT, focusing on the use of connected devices as vectors in distributed denial of service (DDoS) attacks. Through an analysis of the Mirai DDoS, the paper identifies three unique characteristics of IoT botnets: a) higher utilisation rate; b) more durable infections; c) greater contamination rate due to their increasingly connected ecosystem. The paper concludes that an adaptive governance structure is required to effectively respond to the dynamic cybersecurity risks associated with IoT and its potential to develop into a global infrastructure of vulnerabilities. This complex adaptive system cannot be based solely on traditional points of authority (e.g. regulation; formal standards) and relies on the information gathering and monitoring capabilities of transnational internet anti-abuse communities, such as M3AAWG and APWG, to provide a more modular response to the global proliferation of IoT products with low level of security.

Keywords: IoT, cybersecurity, adaptive governance, global private governance

Introduction

The Internet of Things (IoT) is increasingly capturing the attention of policy-makers, businesses, the media and the wider public. Currently, IoT is defined as:

> *"an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react"* (ISO/IEC JTC 1, Working Definition).

In itself, adding communication and sensing capabilities to physical objects is not new, dating back to the late 1990s when products and industrial parts become equipped with radio frequency identification tags (RFIDs) in sectors such as commerce, transport and logistics (IEEE Internet Initiative, 2015; Xu et al., 2014; Brown 2015).

However, in recent years, IoT has proliferated across a wide range of business-to-consumer (e.g. fitness tracking, home security, energy metering) and business-to-business sectors (e.g. monitoring machinery, managing inventory, data analytics). Gartner, the digital market research and analysis company, forecast that "8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016, and will reach 20.4 billion by 2020". Gartner noted that the consumer segment "is the largest user of connected things with 5.2 billion units in 2017, which represents 63 percent of the overall number of applications in use" (Gartner 2017).

Embedding sensing capacity, connectivity and actuation at scale in everyday objects enables new ways of organising social and economic activity. At a basic level, it allows individuals to better understand their consumer behaviour (e.g. smart energy meters) or to control and automate certain aspects of their daily lives (e.g. smart fridges for grocery shopping). In addition, it allows businesses to generate more meaningful insights from their customer data, to better forecast demand and supply (e.g. smart energy grid - smart energy planning) or to potentially enable new patterns of ownership and business models to emerge (e.g. connected and autonomous vehicles – transport as mobility).

However, embedding connectivity in everyday objects and, most importantly, at the scale reported and projected by current market analysis brings about crucial policy concerns, especially with regard to data protection and cybersecurity (OECD 2016, GoScience UK 2015, IEEE-SA 2015). These challenges are most evident in the IoT consumer segment, which has witnessed most growth in recent years.

There are at least three reasons why IoT consumer products have a low level of security and raise increasing concerns over privacy, security and safety. First, the consumer products industry has characteristically operated at low margin, especially with the growth of global supply chains. Adding connectivity to traditionally unconnected consumer products is perceived as a driver to increase sales and profits in this low margin industry faced with increased competition. Thus, manufacturers of IoT consumer products have limited incentives to embed cybersecurity specifications in consumer products, which would increase costs while also potentially affecting the life and user-friendliness of their products (Brown 2015). Second, many of the firms operating in this global supply chain, as well as many of the consumers currently purchasing IoT products, have limited experience of valuing cybersecurity in everyday products such as toys, lightbulbs, fridges. Subsequently, at present, it is difficult for manufacturers, suppliers and consumers to price cybersecurity to the extent that they are currently valuing safety in consumer electronics or motor vehicles. Lastly, even if manufacturers and sellers of IoT consumer products have an incentive to introduce cybersecurity into their products (e.g. for brand reputation), it is difficult and costly for them to push best cybersecurity practices down the entire supply chain and to monitor that they have been adopted by each supply tier, including software and hardware providers (Brass et al 2017).

In this context, IoT compounds the impact of security disincentives in a globally distributed consumer product market that is notoriously high clockspeed and low margin. This results in the release of products with a relatively low degree of security, as manifested in the use of vendor default passwords and lack of interfaces for device owners to update them, as well as limited device capability to identify vulnerabilities and perform software updates. Thus, IoT products with low security specifications act as a target and source of network abuse, increasing the vector surface of compromised devices used for in botnets for Distributed Denial of Service attacks.

The result of these practices is an extreme form of negative spillovers in Internet security: insecure products have costly implications for network providers, regulators and policy-makers, who have to internalize these costs in their operations (e.g. internet providers who monitor the networks for abuse such as botnets) and to construct measures to correct behaviour against them (e.g. regulators/ policy-makers who have to ensure that citizens are provided with a responsible level of data protection and cybersecurity).

This paper conducts an analysis of the Mirai distributed denial of service (DDoS) attacks on KrebsonSecurity, OVH and Dyn using compromised IoT endpoint devices (routers, CCTVs and TV sets connected to the Internet) in order to investigate the unique cybersecurity risks and uncertainties that are emerging from the growth of IoT.

The paper identifies three unique characteristics of IoT botnets. The first is the higher potential utilization rate of permanently switched on, connected things. The second is that infections are more durable given the lack of or limited capacity of these devices to incorporate security features in their hardware as well as control and lifetime vulnerability management in their software. Third, IoT devices have a potentially greater contamination rate due to the increasingly networked ecosystem in which they operate (e.g. smart homes). The result is a malware infrastructure that is more reliable for abusive activities than conventional botnets.

Having identified the unique characteristics of IoT botnets, the paper explores the potential governance mechanisms for managing the risks associated with this technology, focusing on three types of interventions: a) mandatory regulation at domestic level; b) voluntary standardisation at domestic and international level; c) self-regulation by expert anti-abuse communities at international level.

Rather than arguing in favour of a single type of intervention, the paper proposes an integrated and adaptive governance approach that relies on complementarity of interventions and the combined capabilities of domestic and transnational actors to tackle the cybersecurity risks associated with IoT (Abott and Snidal 2009, Buthe and Mattli 2011, Cafaggi 2012b). Risk regulation, whether mandatory or voluntary, has to balance considerations about the degree of anticipation/precaution (i.e. minimising the production of risk) and resilience (i.e. mitigating the effects of hazards) embedded in intervention packages to tackle the low level of IoT cybersecurity. This implies that each of the key dimensions of risk regulation have to be satisfied in order to respond to the negative externalities of releasing insecure IoT products into the global market: a) information gathering; b) monitoring; c) control; d) correction (Table 1).

[Insert Table 1]

The paper concludes that an adaptive governance structure is required to effectively respond to the dynamic cybersecurity risks associated with IoT and its potential to develop into a global infrastructure of vulnerabilities. This complex adaptive system cannot be based on a single point of control or authority. It requires the identification of key nodes of control and their respective resources: a) knowledge/ information; b) human resources; c) financial resources; d) authority to modify behaviour. Transnational anti-abuse communities, such as the Message, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG), play a crucial role in information gathering and monitoring traffic, contributing with intelligence to the governance complex for managing the cybersercurity risks of IoT as well as facilitating a more modular response to these risks than formal regulations or standards for cybersecurity can achieve on their own.

The Mirai Case

The Mirai botnet, and its unprecedented magnitude, is a recent and well-known instance of negative spillovers resulting from a market with limited incentives to design IoT devices with adequate security specifications.

On 30th September 2016, the source code for Mirai was released on HackForum by a user called Anna-Senpai. Mirai is a malware designed to search for and compromise Internet-connected devices that are protected with factory default passwords and usernames, such as poorly secured CCTV cameras, TV sets or routers. The approach was to continuously scan the IPv4 address space for vulnerable devices, typically against destination ports TCP/23 and TCP/2323. It has been reported that “the mean time to compromise a vulnerable IoT device is 10 minutes or less, which means that compromised devices which are switched off or simply rebooted will almost certainly be re-compromised in short order […]” (Dobbins 2016). These devices were then used as a platform to launch DDoS attacks on large-scale networks such as

Dyn and OVH. According to Herzberg et al, Mirai used a “brute force technique for guessing passwords a.k.a dictionary attacks based on the following list” (Figure 1):

[Insert Figure 1]

Given its continuous scanning capabilities, by which a compromised IoT device starts immediate scanning for other devices, Mirai had a floating population of devices located around the world. This allowed for the magnitude of the DDoS attacks on Krebs on Security and OVH. The attack on Krebs was reported at 620Gbps, while the attack on OVH counts as the Internet’s largest DDoS attack at 1Tbps, using over 100,000 devices (Vijayan 2016, Waqas 2016).

Although Dyn has confirmed that the attack targeted at it had the Mirai botnet as primary source of malicious attack traffic, it hasn’t yet confirmed its magnitude or the estimated number and location of the compromised devices. It has, however, indicated that observations of the TCP attack volume from its datacentres indicated “packet flow bursts 40 to 50 times higher than normal”, with some reports estimating an attack magnitude in the 1.2 Tbps range (Hilton 2016). If confirmed, the DDoS on Dyn will become the largest in terms of bandwidth size. After the release of the Mirai code, the cybersecurity software company Imperva conducted a review of recent assaults on its network to identify if any of them carried out Mirai imprints. It found that the Mirai botnet was responsible for a rise in GRE floods mitigated by its services in August, which peaked at 280 Gbps and 130 Mpps and indicated a powerful botnet. Imperva reported that “investigation of the attack uncovered 49,657 unique IPs”, recorded in 164 countries, peaking at 280 Gbps and 130 Mpps (Herzberg et al. 2016). Imperva also revealed the geolocation of the compromised IoT devices at the time of the investigation (Figure 2).

[Insert Figure 2]

In February 2017, Kaspersky Labs released its Q4 2016 DDoS Intelligence Report, confirming that this quarter saw the longer DDoS attack of the year, which lasted for 292 hours (or 12.2 days), and a record-breaking number of DDoS attacks in one day (1,915 launched on 5th November 2016). Kirill Ilganaev, Head of Kaspersky DDoS Protection, predicts that the array of devices being harnessed by botnets are increasingly diverse and target more prominent and bigger networks:

> *"IoT devices have the potential to launch DDoS attacks of any complexity, including application layer and encrypted attacks. Given the effectiveness of IoT botnets, as well as the growing number of poorly protected IoT devices, we can reasonably predict an increase in the number of such attacks as well as their power and complexity. That means companies need to take care of their protection in advance, and take a scrupulous approach to choosing their DDoS attack filtration service"* (Kaspersky Lab, 2017).

The Unique Cybersecurity Vulnerabilities of IoT Devices

The Mirai botnet has unique characteristics with regard to the compromise method, the magnitude and the impact of the attack. Regarding the compromise method, the use of IoT devices to create botnets is considered much easier and cheaper than compromising PCs. Scanning the IP address space for vulnerable devices is much more cost effective than relying on a spam service to phish PC users. Given the current and projected growth of IoT, connecting and networking more things means increasing the number of entry points to a network and, subsequently, increases the likelihood that more connected devices with limited protection will be used in future attacks (Global Sign 2017). However, Vijayan noted that increased competition for vulnerable devices could also lessen the intensity and scale of Mirai-enabled

DDoS attacks, as the same devices could be used to serve a growing number of service denials (2016).

Nonetheless, the simplicity of the compromise method, combined with the magnitude of the attack, reveals the unique cybersecurity challenges of IoT. For instance, Verizon's 2016 Data Breach Investigations Report shows that the mean density of a DoS was 5.51Gbps and 1.89Mpps in 2015 (Figure 3). By contrast, the Mirai botnets reached 280Gbps (Imperva), 620Gbps (Krebs on Security) and 1Tbps (OVH).

[Insert Figure 3]

Taken together, IoT devices have a number of characteristics that increase the strength and complexity of DDoS attacks. IoT consumer devices are: 1) are always on, 2) have no antivirus support and/or limited update mechanisms, making malware development no more challenging than writing another system daemon, 3) do not have fail-safe mechanisms that cut connectivity but preserve baseline function (e.g. an IoT refrigerator that can be taken offline but still perform the basic chilling functions), and 4) are computationally underpowered, but often have a surfeit of raw network interface capacity. Taken together with extraordinarily low barriers to penetration - Mirai had a brute force dictionary of approximately 60 uid/gid pairs - IoT abuse platforms are comprised of elements that have utilization potential much higher than desktop machines, have no performance degradation noticeable to users when infected, and no easy way for the average user to remove the infection.

In short, when leveraged in abuse platforms, IoT botnets have the potential to provide more bang for the abusers' buck. Even worse, unlike visual multitasking environments where user interface and performance lag may be an indicator that a malware infection is awry, IoT devices may not exhibit performance degradation and may only be reparable through a factory reset users may not know how to perform. Even if users had the incentives to take these mitigation efforts, the technical barriers are often higher than applying conventional AV tools.

Thus, IoT botnets bring new challenges for network providers, regulators and policy-makers. The first is the higher potential utilization rate of permanently switched on, connected things. The second is that infections are more durable given the lack of or limited capacity of these devices to incorporate security features in their hardware as well as control and lifetime vulnerability management in their software. Third, IoT devices have a potentially greater contamination rate due to the increasingly networked ecosystem in which they operate (e.g. smart homes). The result is a malware infrastructure that is more reliable for abusive activities than conventional botnets.

Mapping Interventions for IoT Cybersecurity Governance

The market failure in the global supply chain for IoT products raises questions about the type and locus of interventions needed to limit the proliferation and compromise of insecure products. Conventional wisdom argues that a market failure of this magnitude requires government intervention in the form of mandatory regulatory frameworks, which combine the development of a set of minimum security specifications with product certification schemes. Given the global nature of the supply chain for IoT products, and in order to limit the negative impacts of a potential regulatory race to the bottom, these minimum security specifications would also require international harmonisation in standards development organisations (SDOs). In the market for consumer electronics, this approach is currently used to certify the safety and quality of appliances, medical devices or radio equipment.

State-mandated regulations

To date, governments and regulators across the three regions that are estimated to "represent 67% of the overall IoT installed base in 2017" – Western Europe, North America and East Asia – have adopted a 'light touch' regulatory approach to securing IoT, issuing a combination of non-binding, high level guidelines and sector-specific recommendations (Gartner 2017). In other words, governments have to date predominantly utilised their advisory rather than their rule-making capacity to promote IoT security.

This approach has been used in the UK and the US, where government agencies have released minimum guidelines for "security by design" and "security by default" for IoT products and systems. For instance, in the US, the Department of Homeland Security produced a set of non-binding Strategic Principles for Securing the IoT, following an end-to-end and lifecycle approach to IoT security. The principles indicate that "security by design" (i.e. in the technical design of an IoT product or system) needs to be complemented by wider security by default strategies, most notably: a) that security updates and vulnerability management should occur not only through the product lifecycle but also the business lifecycle (e.g. the durability of associated products, the anticipated costs of repair, coordinated disclosure of vulnerabilities), and b) that risk models should be tailored to a device's intended use and environments (US DoHS 2016).

This 'light touch' regulatory approach, which promotes rather than mandates minimum security standards for IoT products, has the benefit of being less intrusive in the product development process and the consolidation of the market. However, this approach has limited effectiveness at monitoring and ensuring compliance with "secure by design" and "secure by default" principles for IoT products as they enter the market.

An alternative approach would be state-mandated regulations similar to the safety rules and certification schemes widely adopted across the world. This approach is currently discussed in the EU, where some EU Member States (e.g. Germany) and the European Commission are considering new regulatory instruments – such as a certification and labelling system – to encourage manufacturers and importers of IoT products who are interested in accessing the EU single market to promote security and to inform consumers about the criticality of their products. A proposed approach is the adoption of a traffic light label akin to food and energy efficiency labelling. A key benefit of this precautionary approach is the minimisation of the proliferation of cybersecurity risk in a given market.

However, given the supply chain for IoT products, it is likely that this approach is less effective at minimising the production of cybersecurity risk at a global scale (Genschel & Werle 1993). Recalling Figure 2, Mirai-compromised IoT devices were identified across the world (i.e. IP addresses of Mirai-infected devices were identified in 164 countries) and, predominantly, in markets that have not yet taken measures to promote a minimum level of device security (e.g. Vietnam, Brazil). This raises questions about the effectiveness of state-based mandatory regulations for IoT devices in the absence of internationally harmonised standards for minimum security specifications.

Voluntary international standardisation

The decentralisation of technical control via standards is a well-documented and recognised form of establishing and disseminating best practice in the supply chain of consumer products, such as electronics (Abbott and Snidal 2001, Buthe and Mattli 2011, Mattli & Buthe 2003).

However, at present, the standards landscape for IoT security is highly fragmented. On the one hand, international industry alliances are producing an increasing number of de facto standards:

Online Trust Alliance (OTA), Open Web Application Security Project (OWASP), Cloud Security Alliance (CSA), GSM Alliance (GSMA), OneM2M. One of the main concerns with the emergence of these standards is that they are driven by market dynamics, causing further fragmentation of the IoT cybersecurity standards landscape, as alliances compete to promote their own technical specifications and principles. In addition, the adoption and implementation of de facto standards is difficult to monitor at a global scale and the current lack of consolidation can, in fact, undermine the incentives IoT manufacturers have to secure their products.

Standards development in formal organisations (e.g. ISO/ IEC, ITU) can achieve the consolidation of security standards for IoT consumer products, given their consensus decision-making processes and their formal approval procedures (. By linking these standards to trade regimes (e.g. WTO rules on product safety), formal standardisation processes could principally achieve the establishment of minimum security specifications for IoT products at a global scale. However, at present, no formal standards for IoT security in consumer products have been adopted by international standards organisations. Although security standards for certain IoT applications have been adopted in ISO/ IEC (e.g. unmanned aerial vehicles), one of the main limitations of formal international standardisation is that it is a long, resource consuming process and the consensus decision-making that is embedded in the work practice of technical committees within these organisations has a direct effect on the timely adoption of global standards.

The Role of Transnational Anti-Abuse Communities

Anti-abuse and network operator communities, such as the Message, Malware, and Mobile Anti-Abuse Working Group (M3AAWG) and the Anti-Phishing Working Group (APWG) have traditionally played a crucial role in identifying and working together to tackle bots, malware, spam, viruses, DDoS attacks and other types of online exploitation. Given that they are on the front line of IoT abuse, they hold essential intelligence and monitoring capacity to inform and support other control and correction agents (e.g. regulators, governments) on the characteristics and scope of compromised IoT products. In addition, anti-abuse and network operator communities have played a crucial role in developing and horizontally implementing anti-abuse norms.

In the world of IP reputation, the anti-abuse community comprises the world's expertise in collecting abuse indicators through feedback loops and information sharing, synthesizing those indicators into reputation metrics, and effectively binding that reputation through firms' application of those metrics at e-mail and traffic gateways around the globe. The anti-abuse community has developed a reputation network that has kept pace with conventional abuse networks and an information sharing network that synthesizes diverse reports of abuse into actionable reputation information, whose demand is demonstrated every day by its ability to protect users from abusive messaging around the world.

Similarly, when abusive actors moved into hosting, an industry typically outside conventional anti-abuse communities, the anti-abuse community recognized these new sources of abuse and actively engaged the hosting industry to develop best common practices. Today, M3AAWG has a healthy relationship with the hosting industry, in particular, the Internet Infrastructure Coalition (i2Coalition) - an industry group comprised of security conscious hosting providers that now contribute to promulgating and developing anti-abuse norms in their community, including through network operator fora such as NANOG.

Given the global character of the internet infrastructure, anti-abuse communities can perform two fundamental roles – information gathering and monitoring - that traditional intervention mechanisms (e.g. state mandated regulations; voluntary international standardisation) cannot fully and effectively achieve given the jurisdictional constraints of regulatory measures, the time constraints of standards development, and their limited capacity to monitor and enforce compliance with a minimum set of security specifications in the global supply chain for IoT products. Given their high clockspeed response mechanisms, anti-abuse communities can serve as a credible source of intelligence on the characteristics and scope of IoT products with low security specifications as well as an adaptive mechanism to ensure that security best practices are dynamic enough to respond to the complex and changing security risks of the IoT market.

Conclusions

The Mirai DDoS attack has revealed a market failure in the supply chain for IoT consumer products and the global scope of IoT cybersecurity risks. Traditional intervention mechanisms for securing IoT, such as state-mandated regulations and voluntary international standardisation, have not yet fully developed. Although effective at controlling and correcting behaviour, such mechanisms take a long time to develop, to build capacity and to be implemented (Abbott and Snidal 2009). In addition, their effectiveness at the global scale can be questioned given the high level of jurisdictional and market competition that characterises the early development stage of the IoT industry. Thus, whereas state-mandated regulations and voluntary international standardisation can be effective precautionary measures, by minimising the production of security risks in the long term, they require considerable time and financial resources to construct robust regimes with international reach, similar to the current international regime on safety in consumer electronics (Abbott and Snidal 2011, Buthe and Mattli 2011). Transnational actors such as anti-abuse communities play a crucial role in providing the necessary information gathering and monitoring capabilities needed to understand the characteristics and scope of compromised IoT devices, to categorise their criticality and assess their impact in order to mitigate the negative effects of current security practices in the supply chain for IoT products (Cafaggi 2012a, 2012b). Anti-abuse communities play a crucial role in the governance complex for securing IoT by providing the system resilience needed to deal with the complex and dynamic development of this market. Thus, rather than focusing on a particular type of intervention, tackling global IoT cybersecurity risks require an adaptive governance system based on the modularity between risk anticipation (e.g. standards, certification schemes) and system resilience (e.g. information gathering, monitoring).

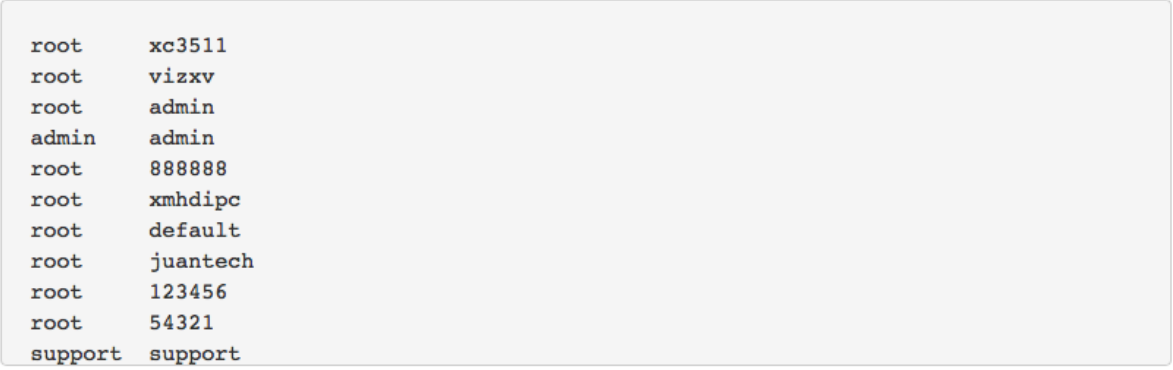
Figures and Tables

Table 1: Dimensions of Regulations for IoT Cybersecurity Governance

Dimensions of Regulation	Types of Intervention	Response to Risk
Information gathering	Voluntary self-regulation	Resilience
Monitoring	Voluntary self-regulation	Resilience
Control	Voluntary self-regulation Mandatory regulation	Anticipation/ Resilience
Correction	Mandatory regulation Enforced self-regulation	Anticipation

Source: Brass et al (2017)

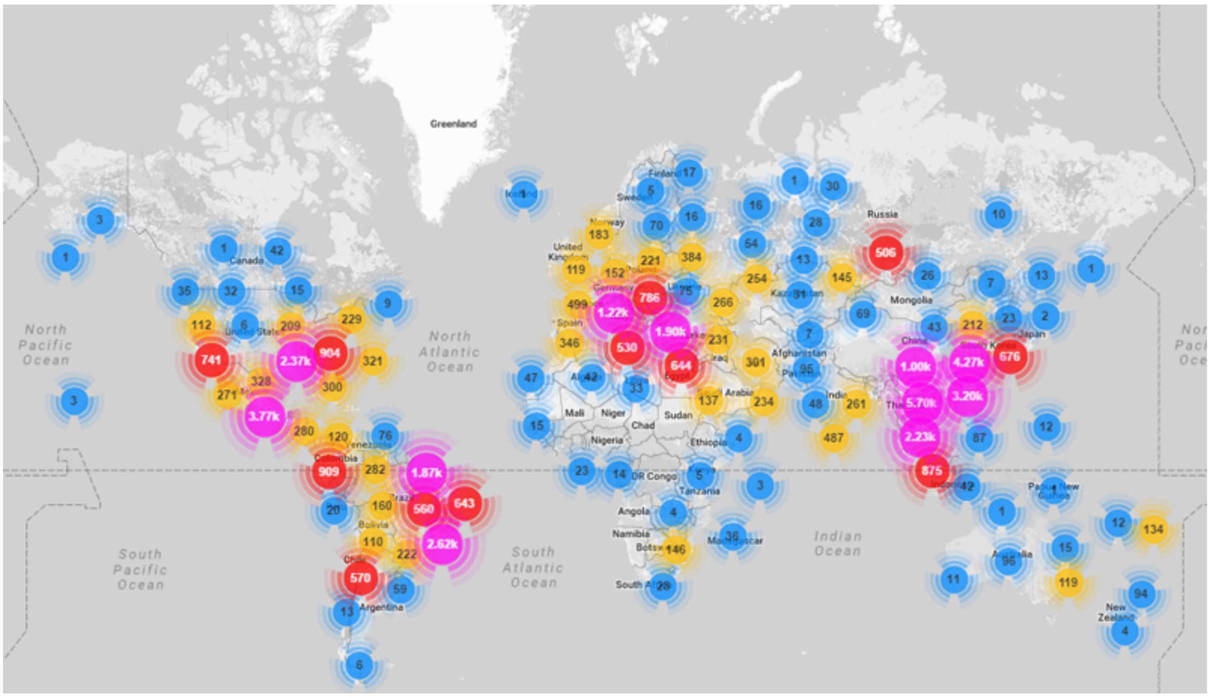
Figure 1: Mirai Technique for Password Guessing



```
root     xc3511
root     vizxv
root     admin
admin    admin
root     888888
root     xmhdipc
root     default
root     juantech
root     123456
root     54321
support  support
```

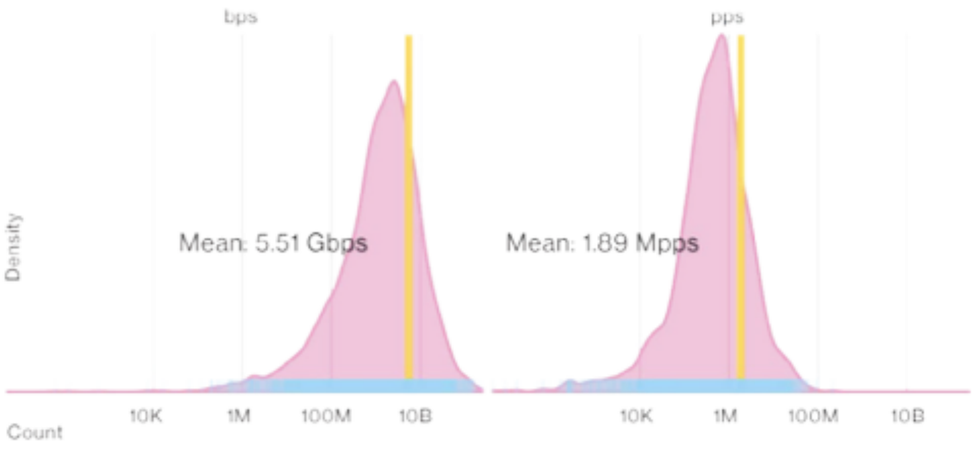
Source: Herzberg et al (2016)

Figure 2: Geo-locations of all Mirai-infected devices



Source: Herzberg et al (2016)

Figure 3: Denial-of-Service Attack Bandwidth and Packet Count Levels (n=10,808)



Source: (Verizon 2016)

Bibliography

Abbott, K. and D. Snidal (2009) The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State, in W. Mattli and N. Woods (eds) *The Politics of Global Regulation,* Princeton NJ: Princeton University Press.

Abbott, K. and D. Snidal (2001) International 'Standards' and International Governance, *Journal of European Public Policy* 8(3), pp 345-370.

Black, J. (2008) Constructing and Contesting Legitimacy and Accountability in Regulatory Regimes, *Regulation and Governance* 2, pp. 137-164.

Brown, I. (2015b). *Regulation and the Internet of Things. ITU GSR Discussion Paper*.

Dobbins, R., 2016. Mirai IoT Botnet Description and DDoS Attack Mitigation. *Arbor Threat Intelligence*.

Buthe, T. and W. Mattli (2011) *The New Global Rulers: The Privatisation of Regulation in the World Economy*, New Jersey: Princeton University Press.

Cafaggi, F. (2014) A Comparative Analysis of Transnational Private Regulation: Legitimacy, Quality, Effectiveness and Enforcement, Preliminary Report, Available at http://www.eesc.europa.eu/resources/docs/a-comparative-analysis-of- transnational-private-regulation-fcafaggi_12062014.pdf, Accessed 10 September 2014.

Cafaggi, F. (2012a) Introduction: The Transformation of Transnational Private Regulation: Enforcement Gaps and Governance Design, in F. Cafaggi (ed) *Enforcement of Transnational Regulation: Ensuring Compliance in a Global World*, Cheltenham: Edward Elgar.

Cafaggi, F. (2012b) Transnational Private Regulation and the Production of Global Public Goods and Private 'Bads', *The European Journal of International Law* 23(3), pp. 695-718.

Cafaggi, F. (2011) New Foundations of Transnational Private Regulation, *Journal of Law and Society* 38(1), pp. 20-49.

FTC (2015). *Internet of Things: Privacy & Security in a Connected World*. [Online]. Available from: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Gartner (2017, 7 Feb) Gartner Says 8.4 Billion Connected "Things" Will be in Use in 2017, Up 31 Percent from 2016, http://www.gartner.com/newsroom/id/3598917

Genschel, P. and R. Werle (1993) From National Hierarchies to International Standardisation: Modal Changes in the Governance of Telecommunications, *Journal of Public Policy* 13(3), pp. 203-225.

Global Sign, 2017. 5 Common Cyber Attacks in the IoT - Threat Alert on a Grand Scale [online]. Available from: https://secure.livechatinc.com/licence/1305162/open_chat.cgi?groups=5&embedded=1&session_id=S1482135574.9551e85e13&server=secure.livechatinc.com#https://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot/ [Accessed 4 Jan 2017].

Government Office for Science (2015) The Internet of Things: Making the Most of the Second Digital Revolution, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

Herzberg, B., Bekenrman, D., and Zeifman, I., 2016. Breaking Down Mirai: An IoT DDoS Botnet Analysis [online]. *Incapsula Blog*. Available from: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html [Accessed 6 Jan 2017].

Hilton, S., 2016. Dyn Analysis Summary Of Friday October 21 Attack [online]. *Dyn Blog*. Available from: http://hub.dyn.com/dyn-blog/dyn-analysis-summary-of-friday-october-21-attack [Accessed 10 Jan 2017].

IEEE-SA (2015). *Internet of Things Ecosystem Study*. New York.

Krebs, B., 2016. KrebsOnSecurity Hit With Record DDoS — Krebs on Security. *KrebsonSecurity*.

Lipson, H., 2002. Tracking and Tracing Cyberattacks.pdf.

Mattli, W. (2001) The Politics and Economics of International Institutional Standards Setting: An Introduction, *Journal of European Public Policy* 8(3), pp. 328-344.

Mattli, W. and T. Buthe (2003) Setting International Standards: Technological Rationality or Primacy of Power? *World Politics* 56(1), pp. 1-42.

OECD (2016) The Internet of Things: Seizing the Benefits and Addressing the Challenges, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En

Prince, M., 2013. The DDoS That Almost Broke the Internet [online]. *Cloudflare Blog*. Available from: http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/ [Accessed 9 Jan 2017].

RCRWireless, 2016. IoT security attacks: A timeline of the internet of things' darkest hours. *RCR Wireless News*.

Scott, C. (2012) Beyond Taxonomies of Private Authority in Transnational Regulation, *German Law Journal* 13(12), pp.1326-1335.

Scott, C. (2010) *Regulating in Global Regimes*, UCD Working Papers in Law, Criminology & Socio-Legal Studies, Paper No. 25/2010, Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1598262.

Sellebråten, M., 2016. Hacked IoT devices behind largest DDoS attack to date [online]. *Enterprise IoT Insights*. Available from: http://industrialiot5g.com/20160928/security/hacked-iot-devices-ddos-attack-tag29 [Accessed 9 Jan 2017].

US Department of Homeland Security (2016) Strategic Principles for Securing the Internet of Things, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Van Eeten, M., Bauer, J.M., Ashghari, H., Tabatabaie, S. and D. Rand (2010) The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989198

Verizon, 2016. 2016 Data Breach Investigations Report.pdf.

Vijayan, J., 2016. IoT DDoS Attack Code Released [online]. *Dark Reading*. Available from: http://www.darkreading.com/denial-of-service-attacks/iot-ddos-attack-code-released-/d/d-id/1327086 [Accessed 5 Jan 2017].

Waqas, A., 2016. Mirai Botnet Linked to Massive DDoS Attacks on Dyn DNS. *HackRead*.

Webber, M. (2014). *The regulatory outlook for the Internet of Things*. 2014. Fieldfisher.

Xu, L. Da, He, W. & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*. 10 (4). p.pp. 2233–2243.