Deloitte.
デロイト トーマツ

Defense Policy and the Internet of Things

Disrupting Global Cyber Defenses

About “Defense Policy and the Internet of Things”

This report examines emerging defense policy challenges arising from the rapid global growth of devices connected to the public Internet, referred to as the “Internet of Things” or “IoT”.

Publicly-available information provided the basis for characterizations of defense policy used in the report. The authors did not have access to non-public information. Data on internet-exposed systems was generated by searches conducted through the publicly-accessible SHODAN search engine (www.shodan.io) using Deloitte-designed queries during September and October 2016. Details of the search method, including specific queries, are provided in the Technical Appendix.

This is an independently-developed report, and no government agencies were involved in drafting or reviewing the contents.

Contents

Executive Summary

Current defense policies in Western nations appear vulnerable to attacks directed against, or emanating from, the fast-growing Internet of Things.

Most existing government cyber resources, policies and procedures appear to be directed toward defense of military and government systems and critical infrastructure, leaving responsibility for the defense of other economically and socially significant targets to private actors which may not have the resources to mount an effective defense.

A few Western economies – especially in Eastern Europe and the Baltic region – appear especially exposed, while others including Russia, Iran and China appear much less vulnerable.
Addressing the defense challenges posed by the IoT seems likely to require more broadly empowered military cyber resources, an expanded effort to set standards and regulate internet-connected products, and a “Whole of Nation” defense policy approach.

New Weapons, New Targets: The Growing Internet of Things

Convenient, Growing…and Vulnerable

Smart devices connected to the internet – the “Internet of Things” (“IoT”) – are making life more convenient, improving factory efficiency, and saving lives. IoT devices include consumer products like home automation hubs, DVRs and network routers, as well as factory automation systems that control machinery, and building automation systems that regulate building climate, manage a variety of functions including power consumption, boilers, emergency failure, water flow, elevators and security access control. The low cost and convenience of IoT devices has produced explosive growth, and recent estimates project that more than 50 billion IoT devices will be connected by 2020[1].

Because these devices are connected to the internet, they can be located and manipulated by malicious actors, as well as by their legitimate operators. The fast-growing IoT poses disruptive challenges for national defense authorities because IoT devices present new kinds of targets, as well as new weapons to threaten economic and physical security.

These disruptive challenges are hard to address with traditional defense policy.

Both the targets and weapons created by the IoT are usually in private hands – they are not owned, operated or even accessible by government agencies. When these privately owned systems are attacked, or used to launch attacks, the economic and political consequences can be severe, and beyond the current authority of national defense agencies to address.

Patterns in Recent Attacks: IoT Is Both Weapon and Target

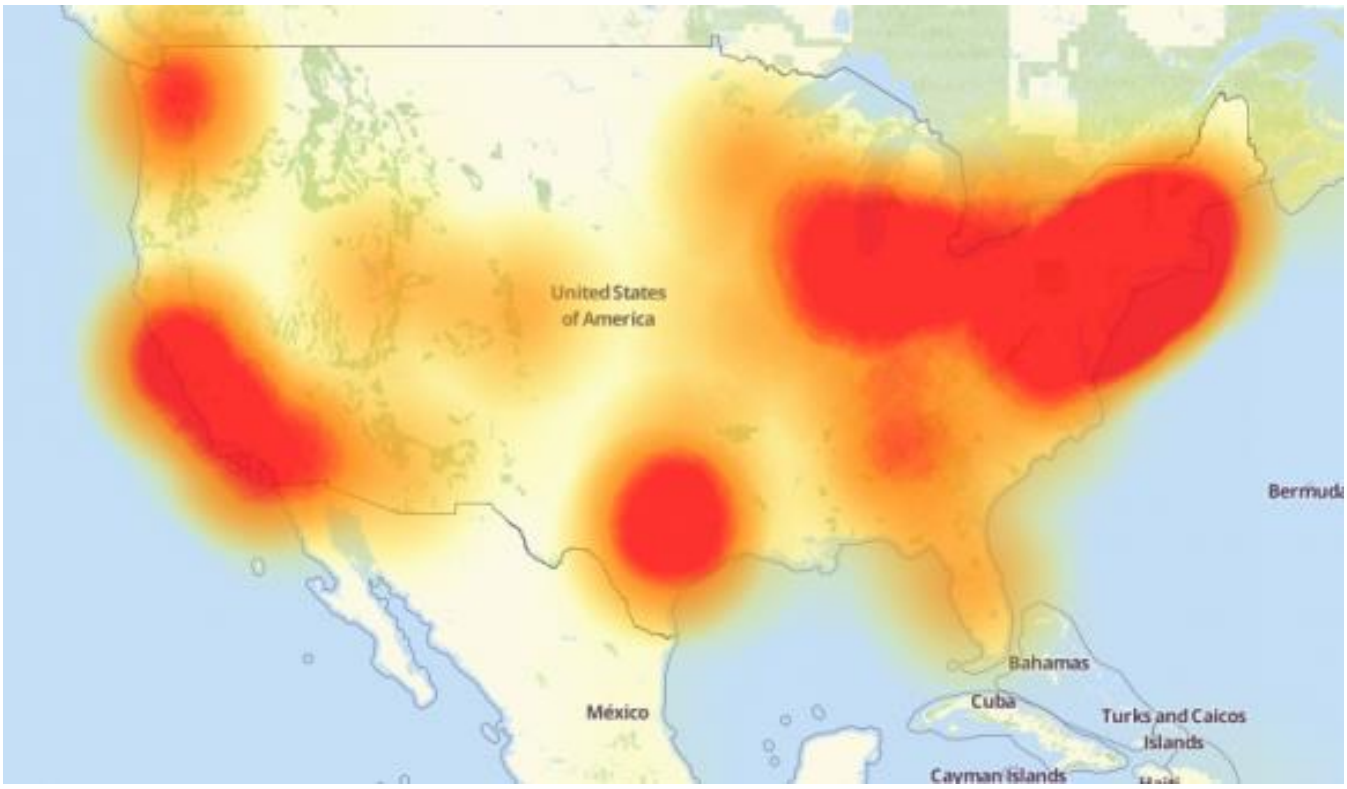
Four recent attacks involving IoT devices show how this emerging technology creates both new targets and new weapons.

1. The Dyn/Mirai Attack: IoT as Weapon

On October 21, 2016, a US company called Dyn (an internet service provider that provides managed domain name service) reported that it was being affected by a massive attack. The attack method used to strike Dyn is called a "Distributed Denial of Service (DDoS)". In this case, tens of millions of internet devices – DVRs, home routers and similar consumer systems – were simultaneously instructed to call Dyn's computers, and to continue doing so indefinitely. The resulting massive overload caused Dyn's services to stop. Dyn's service outage affected millions of US internet users, and caused service disruptions to many popular internet sites including Twitter, Airbnb, GitHub, Reddit and Spotify[2]. Figure 1 below shows the areas of the United States where internet service was denied or interrupted by this single attack.

The attack on Dyn weaponized the Internet of Things, by infecting poorly-protected IoT devices with open-source software called the Mirai Botnet. Mirai infects IoT systems by scanning the internet and attempting to access IoT devices using default usernames and passwords – a common technique in the internet underworld. Although the parties responsible for directing this Mirai-based attack have not been publicly identified, the types of systems used are well-known. Hangzhou Xiongmai Technology, a Chinese technology company, has admitted that its webcam and digital video recorder (DVR) products were used in the assault[4]. Xiongmai subsequently asked its customers to update their device firmware and change usernames and passwords, but few consumers know how to undertake these actions[5].

Figure 1 Areas Affected by the Dyn/Mirai DDOS Attack[3]



2. The Krebs On Security Attack: IoT as Censor

In September 2016, a leading internet security website "Krebs On Security" was the target of a massive Distributed Denial of Service attack which assailed the website with over 600 gigabits per second of "junk" data and caused the site to fail[6]. Attacks on this scale were formerly impossible for all but the most sophisticated actors. However, the Krebs attack – like the Dyn attack – was launched from millions of IoT devices, using Botnet technology similar to Mirai. The timing and form of the attack indicate that a private entity or group of individuals launched the attack, which did not require sophisticated technology or big budgets[7].

3. The PanelShock Exploit: IoT as Target

While IoT devices can be used to launch attacks, they can also present important targets. If malicious actors can take control of IoT systems in factories, office buildings or homes, they can cause damage or disruptions of service. Industrial control systems used to manage factory machinery are critical economic resources, but they may also be exposed to internet-based attacks.

In November 2016, an industry research group announced that it had discovered a significant exposure to attack against a type of industrial control system used to manage factory machinery[8]. Using the internet to access this industrial control system, and applying a well-documented technique called "PanelShock", a malicious attacker can "freeze" a factory control panel remotely and disconnect the panel device from the factory network. This can cause the factory supervisor or operator to perform incorrect actions, further damaging the factory or manufacturing process.

PanelShock is one example of how internet-exposed systems can be captured and damaged, leading to commercial and economic consequences.

4. Finland Freezeout: IoT as Target

In November 2016, the environmental control systems at two apartment buildings in Lappeenranta, Finland were taken down through a Distributed Denial of Service attack[9].

The central heating and hot water systems of the two apartment buildings were controlled through IoT-connected computer systems, and were therefore open to attack. When the attack occurred, the building manager shut the systems down and rebooted them, but the system became stuck in an infinite loop causing the unplanned loss of heat to the buildings[10].

Just as the PanelShock technique allows takeover of internet-exposed factory systems, the attack on the Lappeenranta apartment shows how internet-exposed building automation systems can be damaged, with serious consequences, by remote attacks over the internet.

Which Countries Appear Most/Least Exposed?

National defense authorities are concerned with the exposure of their country to attack, and the Internet of Things represents a new source of exposure. While the IoT is growing and new types of targets are emerging, one way to assess the exposure of a country to attacks against the IoT is to count the number of internet-exposed systems physically located in a country. A comprehensive assessment may not be practical because the number of these systems changes daily. However, a rough snapshot at a specific point in time is possible, even using only open-source search methods.

While new types of systems will arise in the future, present-day IoT targets can be broadly grouped into three sets – building infrastructure, industrial infrastructure and communications infrastructure. A recent search[11] for systems in these three target sets revealed over 130,000 internet-exposed systems (or potential targets) worldwide. The fact that these vulnerable and economically-significant systems can be located using a publicly-available search engine suggests the magnitude of the challenge faced by defense authorities. A simple internet search reveals each system's internet address, key information about the type of hardware and software at the address, and even (in many cases) an invitation to log onto the system.

Figure 2 below summarizes the global search results for the three target sets included in this report. The search results include 49 countries with exposed systems and defense budgets greater than USD 1 billion in 2016. North Korea is not included in this analysis, despite its significant defense budget, because the search methods used in this analysis did not detect any IoT systems inside North Korea. Other countries had exposed systems but do not have significant defense budgets and are not included in this analysis. Other search procedures, searching for other types of systems (e.g. traffic controls, webcams or DVRs) would generate different profiles.

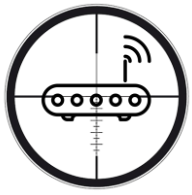
Building infrastructure systems (such as those in the Finland apartment attack) are of defense interest because a large-scale attack on these systems could produce both economic losses and public safety effects. Industrial infrastructure (such as the systems targeted by PanelShock) are also of defense interest because of the potential for economic losses if these systems were attacked on a large scale. Finally, communications infrastructure can be attacked to cause direct economic effects as well as public safety effects. This report did not examine other emerging IoT target sets such as traffic control systems, nor did the search examine national critical infrastructure (major telecommunication switches, nuclear power plants, and other designated national security-related systems).

To assess the relative exposure of national economies to attacks against the IoT targets, a simple index was created by counting the total number of IoT exposed systems in each country, and dividing the total by the dollar value of each country's Gross Domestic Product (GDP) in 2015. The global average exposure was set at a value of 100.

Figure 2 Internet of Things Target Sets

"Internet of Things" Is a Set of Economic Targets

IoT Target Sets
49 Countries with IoT Exposure and Defense Budgets > $1B

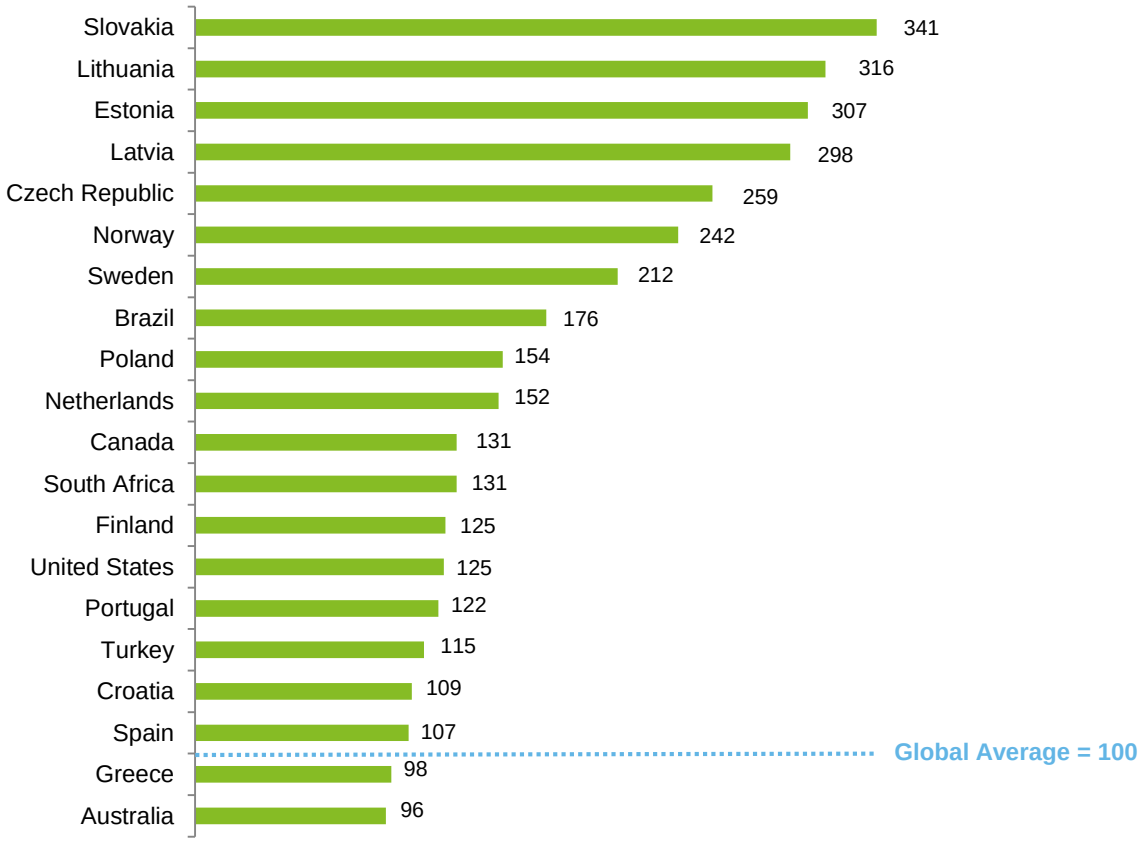
Economic Target Sets	Exposed System Types	Potential Military Effects
 Building Infrastructure > 30,000 Exposed Systems	• Environmental controls • Elevators • Power and lights • Security	• Denial of Access • Physical Damage • Panic and Loss of Confidence
 Industrial Infrastructure > 55,000 Exposed Systems	• CNC Tools • Valves and Switches • Plant Environment • Production Resources	• Lost Production • Asset Damage • Malfunctions/Accidents
 Communications Infrastructure > 37,000 Exposed Systems	• Routers • VoIP Systems	• Loss of Communications • Network Physical Damage • Panic and Loss of Confidence

Source: SHODAN; Deloitte analysis

Figure 3 Most-Exposed Economies

Internet of Things Vulnerability Index

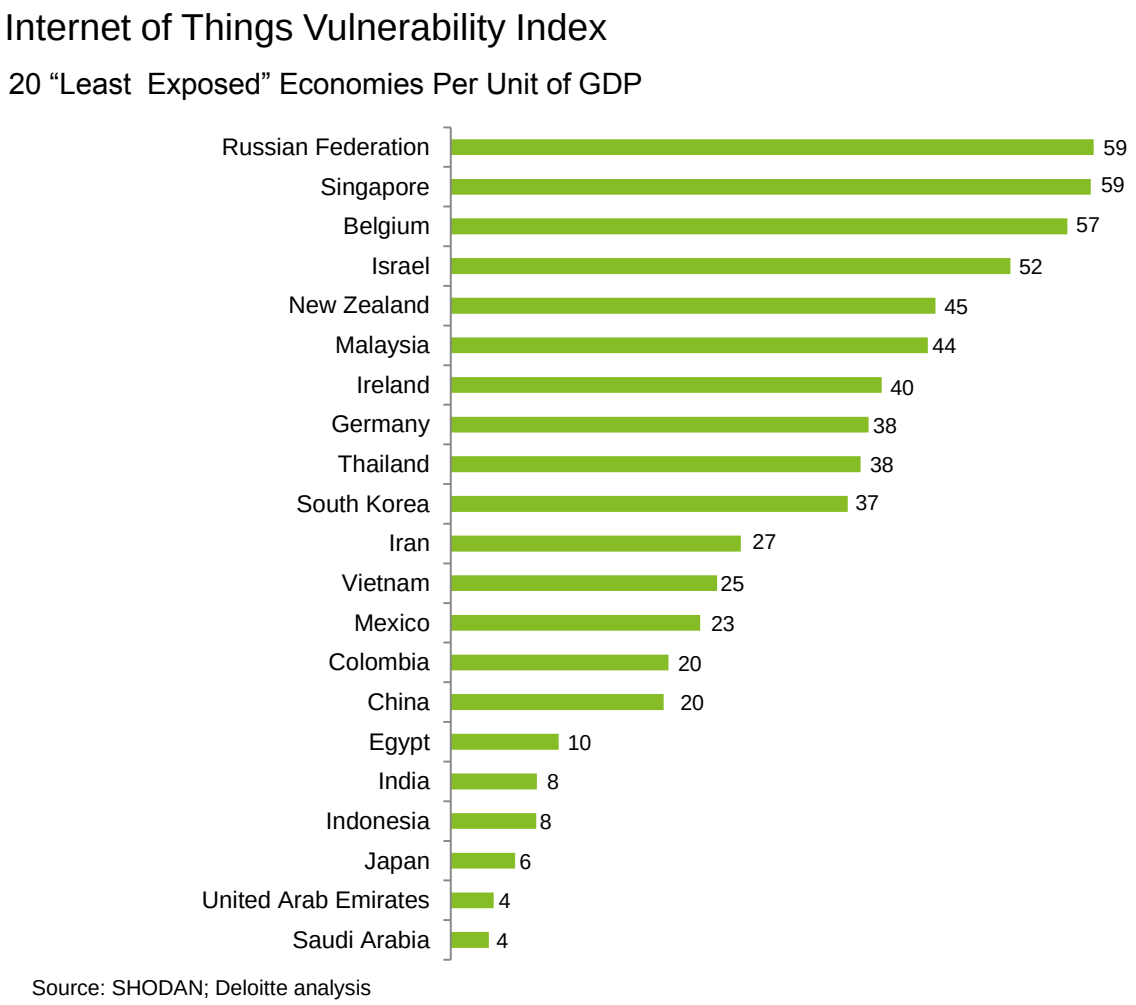
20 “Most Exposed” Economies Per Unit of GDP



Source: SHODAN; Deloitte analysis

Figure 3 shows the 20 most-exposed countries based on IoT targets per unit of GDP. While the US has the largest total number of IoT-exposed systems, adjusting the total number of systems to reflect the relative size of each national economy reveals that the five most-exposed countries are in Eastern Europe and the Baltic region. Businesses and individuals in these countries have adopted IoT systems rapidly, and may have implemented the systems without adequate attention to their level of internet exposure. These five most-exposed economies appear to be more than 2.5 - 3 times more exposed to IoT-based attack than the global average, suggesting that these economies present relatively high risk of economic damage from well-coordinated attacks against the IoT. The United States, while presenting higher-than-average exposure, may be less vulnerable than other developed economies because of the size and diversity of the US economy.

Figure 4 Least Exposed Economies



Source: SHODAN; Deloitte analysis

While the Eastern European and Baltic economies are highly exposed to IoT attack, other countries appear much less exposed. Figure 4 shows the countries presenting the fewest IoT targets per unit of GDP. The least-exposed countries include Russia, China, and Iran – all of which have publicly announced that they are building substantial military cyber capabilities. The difference in relative exposure between most of the European nations and the US (highly exposed) and Russia, China and Iran (less exposed) indicates that there may be short-term incentives for the lower-exposure countries to conduct cyber operations against IoT targets in the high-exposure nations. The incentive arises because it would be difficult for the high-exposure countries to respond in a proportional way to the relatively small target sets presented by prospective adversaries.

Perhaps surprisingly, Japan appears close to the bottom of the list despite its widespread adoption of building and industrial automation. This result may stem from the Japanese practice of custom-building software rather than buying commercially-available tools, or from the practice of isolating these systems from exposure to the internet. In any case, the example of Japan demonstrates that high exposure to the internet is not simply a function of heavy use of automation or economic development – it may reflect a choice about design and implementation methods used for IoT systems.

Unready: Gaps in Defense Policies Worldwide

The Policy Framework: Enabling Effective IoT Defense

Governments make defense policy to set priorities for national defense, establish responsibilities, allocate resources and prescribe the national defense goals and objectives to be reached. To assess the approaches taken by national governments to defense against IoT-based threats, existing national approaches for traditional cyber operations provide a useful framework for analysis.

Most governments with active cyber programs have adopted a three-level description of military operations in cyberspace, ranging from ongoing operations to "detect" potential cyber threats, to actions which "block" the effects of a specific attack, to actions which "respond" to cyberattacks by taking direct action against an attacker.

Detect: Governments establish policy and procedures by which they become aware of actual or impending cyberattacks. These ongoing actions are characterized as the "Detect" phase of cyber operations. The mission during "Detect" is to make the relevant military, law enforcement and other national authorities aware of the nature, scope, targets and potential effects of significant (national-level) attacks against friendly targets. All "Detect"-related actions take place within friendly networks. "Detect" operations end when the appropriate government and non-government authorities are aware that an attack is imminent or underway and make a decision about how to manage the effects. Examples of detection policy and practices include the US Department of Defense practice of monitoring government networks for potential intrusions, and procedures for alerting commanders and civilian leaders when intrusions are detected.

Block: Once an attack is detected, technical methods are applied to end the effects of the attack on the friendly network. These methods and the associated policies are characterized as the "Block" phase of cyber operations. The mission during "Block" operations is to restore the friendly system to its pre-attack state by taking countermeasures within the friendly network to nullify the effects of the attack.

"Block" begins with a decision by designated defense or civilian national authorities to take action against a specific attack. "Block" operations end when the effects of the attack have been nullified. All actions during "Block" operations occur within friendly networks, and are not directed against the attacker or the attacking systems.

Respond: National defense policies provide guidance and management procedures for responding to cyberattacks by taking action against the attacker. The mission during the "Respond" phase is to take actions which impose costs or degrade assets within the hostile network. "Respond" actions may occur within cyberspace or in other domains. Examples of "Respond" actions include counterattacks against a hostile network, economic sanctions, political responses or conventional military operations. "Respond" begins when the appropriate national authorities become aware of an ongoing cyber operation against national assets, and ends when response actions have been approved and carried out.

Sound cyber defense policy enables timely and decisive actions at each level of cyber operations. An effective defense policy regime would allow national authorities to work efficiently through each step in the decision-making cycle and make the decisions required to detect, block or respond to a cyberattack. Military decision-making cycles can be analyzed by applying a modified version of the four-step sequence commonly described as the "OODA Loop" (Orient – Organize – Decide – Act).

Orient: The key "Orient" challenge for defense policy related to the IoT is straightforward – do national defense decision-makers have the authority and tools to become aware that an IoT-based attack is underway, and can they maintain awareness of the attack and its effects until it is resolved? During this critical initial phase of decision-making, the relevant authorities must become aware that a potential decision is required. This requires information, channels, and recipients. For each level of cyber operations, sound orientation policy provides government and private-sector authorities with situational awareness. For example, during the earliest stage of an attack against IoT assets, policy should equip the relevant authorities with the tools and processes required to become aware that an attack may be underway.

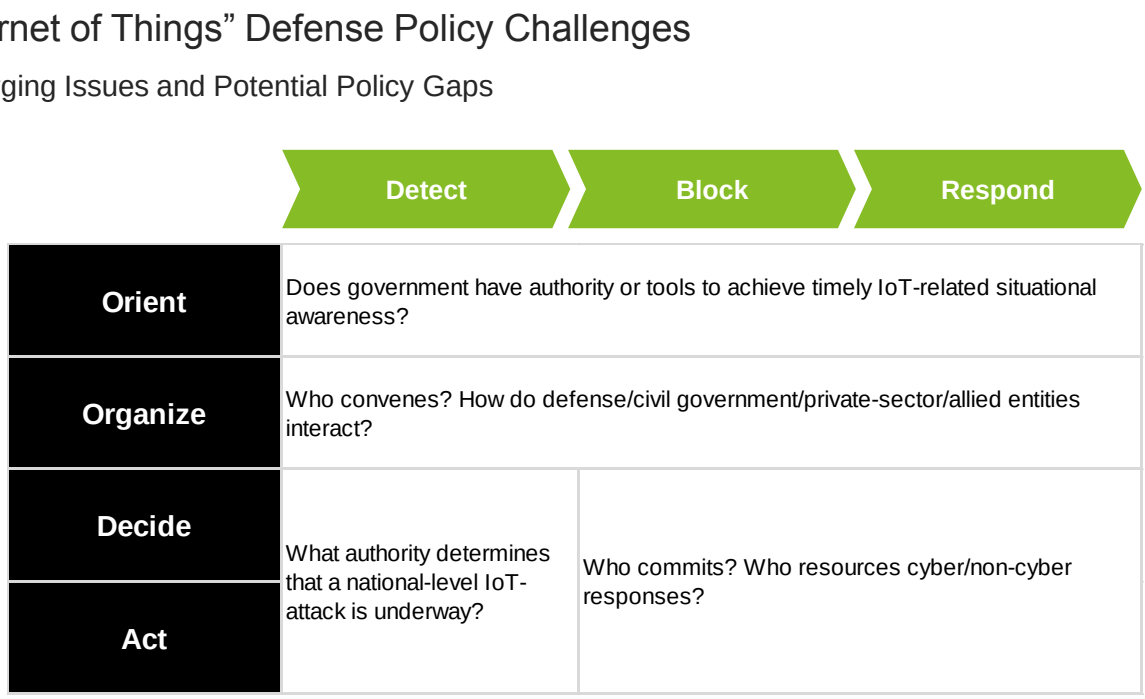
Organize: In this phase, relevant authorities are assembled, made aware of salient facts, and prepare options for decision. During an attack against IoT assets, effective policy would enable key government and private-sector decision makers to convene, provide the information required to generate options (e.g. do nothing, launch blocking operations, or launch a response). To "Organize" at each level of cyber operations, the relevant actors must understand their roles and responsibilities, and be convened in a timely fashion.

Decide: The authorities make a decision which is recognized as legitimate, and orders are given to take some action. Policy should describe decision rules including those required to declare that an attack is underway, to authorize the use of government resources to block the effects of an attack, or to undertake some type of national-level response. For IoT-related decisions, defense policy must define the types of decisions required at each phase of cyber operations and empower national authorities to make decisions which are accepted as legitimate.

Act: The decision is implemented, effects are assessed, and the cycle may repeat if required. Policy should define the authorities and limits to action, the process for making decisions to commit resources, and the responsibilities for implementing decisions and monitoring outcomes.

Figure 5 below shows how the modified OODA Loop and cyber operations framework enable analysis of defense policy for the Internet of Things.

Figure 5 Framework for IoT Defense Policy Analysis



Detecting IoT Attacks

Most current national-level cyber defense policies are focused on detecting attacks against military and government systems and economic assets defined as "critical infrastructure" (e.g. national power grids, telecommunications infrastructure and air traffic control systems). These systems and assets are monitored, and approaches for detecting cyberattacks are well-established. However, detecting even large-scale attacks against IoT targets presents qualitatively different challenges for defense policy. These challenges are of three types – technical, authority-related, and incentive-related.

The technical challenge of detecting attacks directed against the IoT is that the tools used to launch Distributed Denial of Service (DDoS) attacks are difficult to detect and can be emplaced weeks or months before attacks are actually launched[12]. The basic tool used to conduct DDoS attacks is a small software program called a "Bot" (e.g. the Mirai Bot used in the Dyn attack). The "Bot" software can be covertly introduced onto any internet-exposed system (routers, webcams, DVD players or any system within the Internet of Things) and activated on command. Large-scale DDoS attacks occur when large numbers of Bot-infected systems (a "Botnet") are activated and directed against specific targets systems on the Internet of Things.

This method of attack is challenging because the attacker can build up offensive capability over long periods of time, and do so without triggering alerts or alarms.

The technical challenge is further complicated by the authority-related challenge. Most of the millions of systems connected to the Internet of Things are owned and operated by private individuals or organizations. With some exceptions described below, governments are generally not permitted to maintain surveillance of these private systems, even if it were practical to do so. Privately-owned systems such as building automation, factory controls and private communications equipment are exposed to denial of service attacks, but most governments lack authority to detect attacks against them.

Nor do the owners of private systems have any incentive to report attacks to government authorities. Even if an attack is underway, a system owner (for example, the operator of a commercial building) is likely to attempt to mitigate the effects without immediately informing national authorities and risking a public disclosure. This incentive-related challenge further complicates government policy for timely detection of attacks against the IoT. Current government policy approaches underscore the difficulty of detecting attacks against the Internet of Things at each step in the decision making cycle.

Orienting Government Authorities

Most governments have focused cyber policies on the defense of government systems and critical infrastructure, making it difficult for defense authorities to become aware that an attack is imminent or underway. Because governments have little authority to conduct surveillance against private systems, a significant gap in awareness appears to be emerging.

In the United States, Department of Defense policy sets priority on the defense of military networks and civilian Federal government networks[13]. Recent White House directives on cyber policy call for unity of effort and "especially close" coordination between public and private sector entities, but do not provide authority for any government surveillance of IoT systems[14]. The US military is deploying "Computer Emergency Response Team" (CERT) within the National Guard and active-duty forces, but these teams do not have the authority, mission or tools to detect IoT attacks[15].

Other governments appear similarly constrained and ill-equipped to detect IoT-related attacks. For example, Japan's emerging cyber strategy recognizes the growing risk of cyberattacks against infrastructure, as well as attacks on military targets – but does not address the privately-owned assets on the Internet of Things. Because Japan's Self-Defense Forces are integrated with the civil government, Japanese cyber policy is based on a "whole-of-government" approach, and is also closely coordinated with US cybersecurity efforts. Japan and the US made explicit commitments to expand collaboration on cyberspace matters in the 2015 revision to the Guidelines for Japan-US Defense Cooperation[16]. While these measures may facilitate actions once attacks are underway, the IoT detection blind spot still appears in Japanese policy.

Australia recently published a new national cyber strategy which appears to recognize the detection-related challenges presented by the Internet of Things. The new Australian Cyber Security Centre shares threat information with the private sector and is improving its links to critical infrastructure providers[17]. But the Cyber Security Center is not equipped to monitor IoT intrusions and continues to rely on private-sector operators to detect and disclose IoT-based attacks[18]. To share sensitive information quickly with a broader range of businesses, the Australian government plans to establish joint cyber threat sharing centers, co-designed with the private sector, in key capital cities to co-locate businesses and the research community together with state, territory and commonwealth agencies. The Australian strategy also focuses on threat detection through a new layered approach for sharing real time public–private cyber threat information through joint cyber threat sharing Centers.

At the multinational level, NATO's emerging cyber defense policy highlights the gap in authority to detect attacks directed against the Internet of Things. NATO policy emphasizes that the Alliance-level mission is protection of the communication and information systems owned and operated by the Alliance, and that member nations remain responsible for defense of their critical infrastructure and networks. Monitoring or detection activities related to the IoT are not addressed in NATO policy[19].

China has approached the IoT threat detection challenge in a different fashion, reflecting a more interventionist role for the central government in threat detection activity across the full range of internet-exposed systems within China.

While the government's actual ability to implement this policy may be limited, China's cyber policy combines internally-focused measures to increase security of computer systems and insure government access to key systems with externally-focused measures to share information with international partners. Chinese law[20] places heavy requirements on network operators, including government inspection of networks and security measures. The new law does not require a government "backdoor" into sensitive systems, but does require private companies to assist the government with decrypting information. Chinese law requires that core information technology, critical infrastructure and important systems and data must be "secure and controllable" [21] to protect Chinese sovereignty over its cyberspace.

Organizing, Deciding and Acting in the "Detect" Phase

Even if national authorities can be oriented toward detecting an attack against the Internet of Things, existing national and international policy makes timely decision-making difficult. At the most basic level, reaching a consensus that an attack against the IoT is underway requires that national authorities and private-sector stakeholders (including the owners of affected systems) reach consensus on the nature, targets and potential effects of an attack. But the existing policy frameworks adopted by the US, Japan, Australia and NATO do not provide an approach for convening these disparate groups, nor do they set criteria for determining that a national-level attack has been detected.

This is problematic because hundreds of low-level cyber incidents including small-scale denial of service attacks occur daily[22]. Most of these do not rise to the level of national defense challenges, and may in fact be simple criminal acts or even pranks. The difficulties of identifying large-scale IoT attacks, communicating the nature of these attacks to the national authorities, and declaring that a national emergency is underway, have not yet been fully addressed by defense policy.

Blocking and Responding to IoT Attacks

The tasks of blocking and responding to IoT attacks present serious policy challenges at every step of the decision-making process, because the targeted systems are not owned or operated by the national defense authorities.

Orienting and Organizing: Who is Responsible?

When a large-scale attack is underway, blocking actions are the first line of defense. But who is responsible for these actions? Current defense policies call for coordination among public and private stakeholders, but do not fully clarify responsibility or lines of authority.

While every national policy reviewed in this study defines the roles to be played by CERT teams and other military cyber actors during attacks on government systems or critical infrastructure, there are no statements about the roles to be played by national defense assets in blocking or responding to attacks against non-critical privately-owned systems.

This gap may significantly affect decision-making during a large-scale IoT attack. For example, in an attack against building infrastructure systems located in multiple jurisdictions, or even across multiple national borders, what role is played by national defense authorities, and what role is played by the individual building operators? Are blocking actions left to the discretion of each individual operator, regardless of their effectiveness? If national defense resources are requested (or required), what authority do they have to take actions on privately-owned systems? If (for example) a military CERT damages a privately-owned information system, or spills data, who is liable for the damage?

Current US policy highlights the risks of a disjointed effort during an attack on the IoT. The US policy carves up responsibility for the national level response. The Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, is designated as the Federal lead agency for "threat response" activities. At the same time, the Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, is designated as the Federal lead agency for "asset response" activities. The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the Federal lead agency for intelligence support and related activities[23].

The effect of this policy is to involve two Cabinet departments (not including the Department of Defense), the intelligence community, and multiple Integration Centers in a massive coordination effort to determine the best national response to a large-scale cyberattack.

Japanese policy appears to take a more integrated approach, while assigning primary responsibility for blocking and response to private-sector actors. In Japan, the Chief of the Cybersecurity Strategic Headquarters is tasked with "recommending" appropriate responses to cyberattacks including IoT-based incidents. However, Japanese policy recognizes that "cyberspace is built and operated by actors of the private sector as the main driving forces", and requires that the government will "implement policies to catalyze (the private sector's) self-motivated activities and their own initiatives"[24].

Chinese policy for blocking or responding to IoT threats is less encumbered by the public sector/private sector challenges facing other governments. China's 2016 cyber law is clear about the role of the People's Liberation Army and the central government in managing threats directed against any Chinese information system. The new law[25] requires that Chinese network operators shall formulate emergency response plans for network security incidents, and when network security incidents occur, immediately report to the relevant government departments. Responsibilities are further clarified in the 2016 Counter Terrorism law, which requires system operators to provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of "terrorist activities" (such as an IoT attack). While China's ability to fully implement these measures is not known, the responsibility and authority of the central government in managing blocking and response actions has been clearly established in law.

The Open Window

Western governments have focused cyberspace defense policy on protecting military and government systems and critical infrastructure. Defense of privately-owned non-critical systems has been left largely to the owners and operators of these systems. While this approach may have been suitable for computer systems on the commercial internet, the proliferation of IoT systems, and the increasing reliance on these systems for important commercial, industrial and public functions, has created an open window through which attackers can create economic and social impacts which cannot be readily addressed by current national defense policies.

This open window appears to exist at every level of cyber operations. US and European defense policy does not promote early awareness of attacks against IoT targets outside the designated critical infrastructure. Once attacks are underway, policy does not define responsibilities or authorities for blocking or responding to the attacks, relying instead on informal "coordination" and multiple competing bureaucracies to develop the required actions.

The US and European approaches stand in sharp contrast to Chinese cyber policy, which asserts an overriding state interest in maintaining awareness of potential attacks, and places responsibility for responding to attacks squarely with the central government and PLA.

A Way Forward: The "Whole of Nation" Approach

How can defense policy begin to address the challenges raised by the expanding Internet of Things?

Three elements will likely be required to begin adapting to this new domain.

The Military Cyber Basis

Military cyber capabilities are currently directed toward defense of military and government networks and specially-designated critical infrastructure – an approach that appears misaligned with the increasing economic importance of the Internet of Things.

Military involvement in cyber defense is challenging when the targets are civilian systems (i.e. Dyn). The US Posse Comitatus Act[26] forbids the US military from conducting operations that enforce the laws of the United States, except under the express direction of Congress. The Act does not apply to US National Guard in State active duty (which allows National Guard CERT teams to operate inside the US when authorized by state governors), and has been relaxed to allow certain types of operations including those involving nuclear materials or weapons of mass destruction[27].

No authorities have been extended to allow military cyber assets to be applied to detect, block or respond to attacks against civilian IoT targets, meaning that national defense against these attacks is effectively outside the responsibility of military authorities.

Prior to attacks, the US National Security Agency (NSA) focuses on cryptology including both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services designed and developed to enable Computer Network Operations (CNO). These products and services may be made available to civilian agencies and others, but NSA authority does not extend to direct responses to IoT attacks[28].

As response to IoT vulnerability becomes more urgent, it is possible that military authorities could be extended to improve detection, blocking and response to IoT-based attacks. Aside from the legislative and policymaking challenges, using military resources for detection or attribution of IoT attacks would raise serious concerns about privacy and liability. But future circumstances may warrant that the national defense apparatus needs to be adapted to new threats against national economic assets.

Industry Standards and Regulation: The Underwriters' Laboratories Approach

When tens of millions of devices can be hijacked to run the Mirai Botnet, and hundreds of thousands of building and factory automation systems can be identified through simple internet searches, it seems clear that attention should be paid to the products being produced for connection to the internet of things. If devices cannot be detected or easily accessed, then Distributed Denial of Service attacks are more difficult to conduct.

To reduce the vulnerability of economies to IoT-based attacks, security may be improved through adoption of standards and regulations, similar to those for other types of consumer products. This approach is already gaining traction, as the European Commission is developing new legislation to protect machines from cybersecurity breaches, and by creating rules that force companies to meet internet security standards and go through certification processes before being connected to the internet[29]. The European Commission approach may include a labelling system for internet-connected consumer devices that are considered approved and secure.

While this approach is intended primarily for consumer products, a similar standards and certification approach may be useful in limiting the internet exposure of building infrastructure and industrial infrastructure. The example provided by Japan's relatively low level of internet exposure, despite Japan's heavy adoption of automated systems, indicates that the goal is achievable. If these standards are to be developed, national-level legislation or executive actions may be required to establish standard-setting processes and authorities. These processes might usefully embrace a whole-of-nation approach, combining national and municipal civil authorities, defense ministry, military and industry perspectives.

"Whole of Nation" Policies for Detection, Blocking and Response

The Internet of Things presents a qualitatively new defense challenge, because both weapons and targets are civilian-owned, widely-distributed and embedded deeply within the national economic infrastructure. Current defense policies and practices are generally designed to deploy military resources against foreign threats, and policymakers struggle to adapt these policies even to the domestic challenges of physical terrorist acts.

If national defense policy is to address the new challenges posed by the Internet of Things, then it may be necessary to broaden existing joint and interagency planning approaches into a more comprehensive "Whole of Nation" approach. Such an approach is familiar in other spheres, where it is sometimes called "Public-Private Partnership" (as with Japan's approach to domestic disaster relief). Japan is applying its sophisticated model of public-private collaboration to develop policy for non-critical systems on the Internet of Things[30]. The Japanese National Center of Incident Readiness and Strategy for Cybersecurity (NISC) has taken the lead in bringing together public and private entities for the creation of comprehensive security requirements for the design, development and operations of IoT systems[31].

In the case of IoT defense, a "Whole of Nation" approach would address each phase of cyber operations (Detect – Block – Respond) and each step in the decision-making cycle (Orient – Organize – Decide – Act) by applying the optimal private and government resources. For example, detection of a large-scale Distributed Denial of Service attack against building infrastructure in multiple cities or countries might best be done by a coordinated effort among local police and emergency responders, integrated at the national level by an appropriate authority. Timely detection of such attacks might have a deterrent effect, especially if detection could be combined with attribution of the attack to a specific actor.

Such an effort would require closely-integrated action by military, intelligence, police and commercial stakeholders – a complex and high-value activity that would require detailed design and frequent exercises.

There is ample precedent for this type of "Whole of Nation" response, found in (for example) drinking water contamination response protocols or the US Federal Emergency Management Agency (FEMA) Nuclear/Radiological Incident Response plans , although these are primarily designed to manage interagency coordination at the Federal level.

As the threat posed by IoT attacks continues to increase, national policies will need to adapt as rapidly as the threats, and it seems likely that the required adaptations will not respect existing agency boundaries, policies or practices.

Authors

Rieko Arashi
Tokyo
rarashi@deloitte.com

Rieko serves global defense clients working directly with senior operating executives on complex projects requiring both extensive analytical insight and effective inter-cultural communications. Her quantitative analytical skills were honed at University of Chicago, where she obtained her master's degree, Harvard, MIT and Nomura Securities.

Jack Midgley
Tokyo
jackmidgley@deloitte.com

.

Jack focuses on strategy and policy challenges confronting Ministries of Defense and global defense companies. Jack served in Afghanistan as an Army civilian senior advisor to the Commander, International Security Assistance Forces (ISAF). He graduated from West Point, earned the M.P.P. at Harvard and Ph.D. in political science at MIT.

Line Fly Pedersen
Copenhagen
lfly@deloitte.dk

Line is a social scientist trained at University of Copenhagen and Columbia University. She works with welfare- and defense-related clients. She has served Danish clients and international organizations, including the UN and NDI, and done an internship at NATO Headquarters for the Danish Ministry of Defense.

James Pelczar
Tokyo
jpelczar@deloitte.com

Jim focuses on systems security engineering matters brought about by disruptive technologies. He is a former R&D program manager for the US Department of Defense, has bachelor's and master's degrees in engineering.

Amanda Hillock
Wellington
ahillock@deloitte.com

Amanda helps clients make smart investment decisions. This includes business case support, investment advisory, strategic finance and financial modelling across government and commercial sectors, including defense and education. Amanda holds degrees in Economics and International Relations from Victoria University of Wellington.

Gerhard Rickert
Tokyo
gerickert@deloitte.com

Gary focuses on global information security program management, Red Teaming, IT audit and regulatory compliance, and conceptual and creative security design. His current work includes re-thinking approaches to cybersecurity and risk for Japanese and global organizations.

Soren Jones
Tokyo
sorjones@deloitte.com

Soren is a senior consultant in Deloitte Digital. Soren serves global clients developing new customer experiences and ways of interacting with data through advanced technology. He works on making data usable and useful to improve people's lives.

Louis Witcomb Cahill
Auckland
lwitcombcahill@deloitte.co.nz

Louis serves defense clients as a business analyst in Deloitte's Strategy and Operations practice. He holds a Bachelor of Laws and Bachelor of Arts conjoint degree from the University of Auckland, and is a Barrister and Solicitor of the High Court of New Zealand.

Authors acknowledge the contributions and support provided by Tim Denley (Tokyo), Keiko Kameda (Tokyo), Rebecca Kapes Osmon (Austin), David Lovatt (Wellington), Halvor Moen (Oslo), Anu Nayar (Wellington), Elizabeth Nelson (Arlington), Harry Raduege (Arlington), Thomas Riisom (Copenhagen), Phil Sandford (London), and Gen. Chuck Wald (Arlington) and many global Deloitte colleagues.

Endnotes

1. "IoT Growing Faster Than the Ability to Defend It," Scientific American (October 26, 2016), available at https://www.scientificamerican.com/article/iot-growing-faster-than-the-ability-to-defend-it/ (accessed November 29, 2016).

2. "How to defend against the internet's doomsday of DDoS attacks," ZDNet (October 24, 2016), available at http://www.zdnet.com/article/how-to-defend-against-the-internets-doomsday-of-ddos-attacks/?ftag=TREc64629f&bhid=24610997551674372985815076772389 (accessed November 29, 2016).

3. Figure from downdetector.com, available at www.downdetector.com (accessed November 29, 2016).

4. Supra note 2.

5. Supra Note 2.

6. "Why the silencing of KrebsOnSecurity opens a troubling chapter for the 'Net," arsTECHNICA (September 23, 2016), available at http://arstechnica.com/security/2016/09/why-the-silencing-of-krebsonsecurity-opens-a-troubling-chapter-for-the-net/ (accessed November 29, 2016).

7. Ibid.

8. "PanelShock: Schneider Electric Magelis HMI Advanced Panel (0-Day Vulnerabilities)," CRITIFENCE (n.d.), available at http://www.critifence.com/blog/panel_shock/ (accessed November 29, 2016).

9. "DDoS Attacks on Apartments' Heating System Left Residents Cold and Angry," HACKREAD (November 8, 2016), available at https://www.hackread.com/ddos-attacks-on-apartments-heating-system/ (accessed November 29, 2016).

10. Ibid.

11. Deloitte conducted this search in September and October 2016 using the Shodan commercial internet search engine to identify targets in each set. Refer to the Technical Appendix to this report for details.

12. According to Ponemon it takes an average of 170 days to detect an advanced attack, and that appears to apply to conventional devices. See: Ponemon Institute, "Blog," (n.d.), available at http://www.ponemon.org/blog/new-ponemon-study-on-malware-detection-prevention-released. Further analysis by the INFOSEC Institute suggests that latency periods can exceed 200 days; see "Advanced cyber attacks can now nest inside a network for more than 200 days on average before being discovered." http://resources.infosecinstitute.com/the-seven-steps-of-a-successful-cyber-attack/ . (accessed November 29, 2016). Other sources cite lower latency periods, with some caveats; see for example: Mandiant Consulting, "M-TRENDS 2016," (February 2016), available at https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf (accessed November 29, 2016).

13. US Department of Defense, "THE CYBER STRATEGY," (April 2015), available at http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed November 30, 2016).

14. The White House, "Presidential Policy Directive -- United States Cyber Incident Coordination," (July 26, 2016), available at https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (accessed November 30, 2016).

15. See Department of Homeland Security "US-CERT" (no date) available at https://www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

16. Japan Ministry of Defense, "Joint Statement of the US-Japan Cyber Defense Policy Working Group," (May 30, 2015), available at http://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf (accessed November 29, 2016).

17. Australia Government, "Australia's Cyber Security Strategy"(2016) available at https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

18. Ibid.

19. North Atlantic Treaty Organization "NATO Policy on Cyber Defense" (July 2016) available at http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf

20. China's draft cybersecurity law was circulated in July 2015; an English translation is available at China Law Translate, "Cybersecurity Law (Draft)," (July 6, 2015), http://chinalawtranslate.com/cybersecuritydraft/?lang=en#_Toc424040668 (accessed November 30, 2016); China's national security law was passed on 1 July 2015; an English translation is available at "National Security Law," (July 1, 2015), http://chinalawtranslate.com/2015nsl/?lang=en (accessed November 30, 2016); Cyber provisions of China's recently-passed antiterrorism law were reported at NBC News, "China Passes Anti-Terror Law With Controversial Cyber Provisions," (December 28, 2015), http://www.nbcnews.com/tech/tech-news/china-passes-anti-terror-law-controversial-cyber-provisions-n486756 (accessed November 30, 2016).

21. Ibid.

22. Distributed Denial of Service (DDOS) attacks are considered a daily occurrence. One source for live tracking of DDOS reports is available at http://www.digitalattackmap.com/

23. Supra note 12.

24. Japan's National Center of Incident Readiness and Strategy for Cybersecurity, "Cybersecurity Strategy," (September 2015), available at http://www.nisc.go.jp/eng/pdf/cs-strategy-en-booklet.pdf (accessed November 30, 2016).

25. China Law Translate, "Cybersecurity Law (Draft) (Second Reading Draft)," (July 4, 2016), available at http://chinalawtranslate.com/cybersecurity2/?lang=en (accessed November 30, 2016)

26. The Posse Comitatus Act is 8 U.S. Code § 1385 – "Use of Army and Air Force as posse comitatus" available at https://www.law.cornell.edu/uscode/text/18/1385 (accessed November 30, 2016).

27. See U.S. Northern Command's explanation at "The Posse Comitatus Act" (May 16, 2013), available at http://www.northcom.mil/Newsroom/Fact-Sheets/Article-View/Article/563993/the-posse-comitatus-act/ (accessed November 30, 2016).

28. Digital Guardian, "Strangest Things: Defending Against the Future of IoT DDoS Attacks" (October 27, 2016), available at https://digitalguardian.com/blog/strangest-things-defending-against-future-iot-ddos-attacks (accessed November 30, 2016).

29. EurActiv.com, "Commission Plans Cybersecurity Rules for Internet-Connected Machines" (October 5, 2016), available at https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/ (accessed November 30, 2016).

30. Palo Alto Networks, Inc., "Assessing Japan's Internet of Things (IoT) Security Strategy for Tokyo 2020" (September 19, 2016), available at http://researchcenter.paloaltonetworks.com/2016/09/cso-assessing-japans-internet-of-things-iot-security-strategy-for-tokyo-2020/ (accessed November 30, 2016).

31. Japan's National Center of Incident Readiness and Strategy for Cybersecurity, "General Scheme concerning Safe IoT System Security" (August 26, 2016), available at http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf (accessed November 30, 2016).

32. US Environmental Protection Agency, "Drinking Water and Wastewater Utility Response Protocol Toolbox" (n.d.), available at https://www.epa.gov/waterutilityresponse/drinking-water-and-wastewater-utility-response-protocol-toolbox (accessed November 30, 2016).

33. U.S. Federal Emergency Management Agency, "Nuclear/Radiological Incident Annex" (n.d.), available at https://www.fema.gov/pdf/emergency/nrf/nrf_nuclearradiologicalincidentannex.pdf (accessed November 30, 2016).

Technical Appendix

IoT Data Collection Procedure

Counts of internet-exposed IoT systems were generated using the following procedures to search on www.Shodan.io. Eleven searches were conducted on Shodan, grouped into three categories.

1. Communications Infrastructure
(1) port:23,161 vsat
-Telnet and SNMP accessible Very Small Aperture Terminal (VSAT) satellite communications systems
(2) product:voip
-Voice over Internet Protocol (VoIP) devices

2. Industrial Automation
(1) category:ics -icmp -http -html port:102 -product:conpot
-Siemens S7 systems (used in manufacturing and process industries)
-Excluding Conpot honeypots
(2) category:ics -icmp -http -html port:502 -product:conpot
-Modbus protocol (used in industrial control systems)
-Excluding Conpot honeypots
(3) category:ics -icmp -http -html port:2455 operating+system
-CODESYS programming interface (used in industrial automation)
(4) category:ics -icmp -http -html port:9600 response+code
-OMRON Factory Interface Network Service
(5) category:ics -icmp -http -html port:44818
- EtherNet/IP (used in manufacturing automation)

3. Residence & Building Automation
(1) category:ics -icmp_-http_-html port:1911,4911 product:Niagara
- Niagara framework by Tridium (used in building automation systems)
(2) category:ics -icmp -http -html port:47808
- BACnet communications protocol (used in building automation and control networks)
(3) i.lon -title:streetlight.vision
- VisSonic Powerlink (home security and control solution)
(4) Powerlink
- Echelon SmartServer (controller, router, and smart energy manager)

For each category, we downloaded the search results as newline delimited JSON (NDJSON) files, collated the results, and counted the number of unique IP addresses per country.

The data used in the paper were extracted with Python; however, the following R produces the same results for a category, given downloaded NDJSON files for search results at filepath1, filepath2, etc.

```
library(data.table)
library(ndjson)

# Make a list of JSON search result file paths for a category
category.files <- c('filepath1', 'filepath2')

# Read all the search result files for the category into a list of data tables
category.results.list <- lapply(category.files, stream_in)
# Collate the list of data tables into one data table
category.results.collated <-
  rbindlist(category.results.list, use.names=TRUE, fill=TRUE)

# Count the number of unique IP addresses per country
category.results.counted <-
  category.results.collated[,
                            .(count=uniqueN(ip_str)),
                            by=location.country_code]

# Optionally sort the counted results
category.results.counted[order(-rank(count))]
```

Deloitte.
デロイト トーマツ