“Critical infrastructures protection: the responsibility of Government or of companies?”

-

delivered to the Joint Committee on the National Security Strategy

Ben Goldsworthy, 33576556
Computer Science BSc

Abstract

Critical infrastructure is vital to the safety and comfort of the people of the nation—of your constituents. However, as more and more critical infrastructure system have ICT elements implemented into them, the vulnerability of the system (and thus, the nation) to cyber attacks increases. Much of this critical infrastructure is privately-owned, but its security is obviously of much interest to the government. Who, then, should be responsible for this? In this short paper I argue that private businesses should be left to manage their own affairs, but that government would be well-advised to develop and fund nationwide educational and accreditation programmes that can draw upon the wealth of experience and unparalleled access afforded to it through sub-bodies such as GCHQ and help to ensure that those affairs are being managed appropriately.

1 Introduction

Critical national infrastructure (CNI) refers to, as per the Centre for the Protection of National Infrastructure (CPNI), '[t]hose critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life', [1] whilst *critical infrastructure* (CI) is the subset of that CNI that relates to a given area or group of people—for example, the critical infrastructure around Chairwoman Beckett's Derby South constituency. Some have put the percentage of CNI that is privately-run as high as 80%. [2] With this straddling of the boundaries between private business and government, we are led to something of a grey area as pertains to who is ultimately—or rather who *should* be ultimately—responsible for the security and protection of this CI.

It is in both parties' best interest to pass on as much responsibility as possible to the other—this lowers costs for them and protects them from the majority of blame in the event of an incident. However, the fact that this is critical *national* infrastructure suggests that it is critical to the running of the nation. When the nation's government no longer has a function nation to govern, they traditionally don't fare particularly well.

However, the weight of responsibility can obviously not fall solely upon government's shoulders. When they accept the lucrative contracts to provide their services to HM Government, private firms are entering into a partnership in which it is assumed that they shall keep their own house in order.

Ultimately, a hybrid approach is necessary. Government and private industry have their own strengths, and by focusing on each can provide a robust and secure network of critical national infrastructure for the foreseeable future, whilst keeping costs to reasonable levels.

2 Background

There is a slowly growing realisation—at the level of government—of the prevalence within CI of cyber systems, and the vulnerabilities emerging thereof. The Americans realised back in 1998 that '[a]ddressing these [cyber security] vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security', [3] whilst the UK government has been somewhat slower off the bat.

In its *National Security Strategy and Strategic Defence and Security Review 2015*, HM Government recognised that the 'volume and complexity of cyber attacks against the UK are rising sharply, as are the costs to business' [4] and pledged to 'invest 1.9 billion over the next five years in protecting the UK from cyber attack' [4].

A year later, they published their inaugural *National Cyber Security Strategy 2016–2021* (NCSS). It identified that '[t]he future of the UK's security and prosperity rests on digital foundations' [5] and that '[t]he cyber security of certain UK organisations is of particular importance because

a successful cyber attack on them would have the severest impact on the country's national security.' [5]

The NCSS also provisioned establishment of a National Cyber Security Centre (NCSC), which opened just this February. It serves as a consolidation of various antecedent cyber security bodies such as CESG and CERT UK and operates under the auspices of GCHQ. The aim of the NCSC is to 'work together with U.K. organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management[,] underpinned by world-class research and innovation.' [6]

However, the NCSS is also at pains to delimit where it believes the responsibility for security lies, stating that '[n]either the Government nor other public bodies will take on the responsibility to manage this risk for the private sector, which rightly sits with boards, owners and operators.' [5] That said, the government pledges to '[...]provide support and assurance proportionate both to the threat these companies and organisations face, and to the consequences of their being attacked.' [5]

There are a number of important case studies of what can happen when CI is left insecure. One of the most famous of these is commonly known as Stuxnet, called by some a 'cyber weapon of mass destruction.' [7] The Stuxnet malware—introduced to the systems via infected USB flash drives—subtly altered the spin rates of centrifuges within Iran's Natanz Nuclear Power Station, whilst simulteneously feeding a stream of invalid data to the systems responsible for monitoring them. The attack caused the centrifuges to deteriorate over time, eventually leading to a complete breakage. Stuxnet is widely considered a nation state-sponsored attack on the part of the US and Israeli governments and can demonstrate the risk that well-funded and technically-apt adversaries can pose to a nation—for reference of the possible impact of a nuclear power plant disaster, look only to the Chernobyl disaster of 1986.

Another relevant example is the 2015 Ukrainian blackout, which occurred deep into the Crimean conflict with Russia. [8] Large swathes of Ukraine's power grid went out in the middle of winter and brought sections of the country to a standstill in what is considered the first instance of a cyber attack on a country's electricity infrastructure, showing that these threats are always evolving and reinforcing the need to be constantly on-guard. For reference, a similar-length blackout over the London area would cost upwards of £350,000,000.

The scope of these attacks is limitless, and advances in technology are feeding potential attackers with increasing levels of power. [9] Take the following quote from Alex Gibney's 2016 documentary *Zero Days*: 'Let's say you took over the control system of a railway. You could switch tracks, you could cause derailments of trains carrying explosive materials—what if you were in the control system of gas pipelines, and when a valve is supposed to be open it was closed and the pressure built up and the pipeline exploded?" [10] Such an attack may also be merely the start of a problem—'[a] cyber attack on national infrastructure may be an end in itself[...]or it might be a precursor to an overt act of war.' [11]

3 What must be (and what is being) done?

As the NCSS outline, private firms are to be given responsibility for the security of the systems within their remits. However, it would be unwise to simple take such businesses at face value (*Eyes passim ad nauseum*) and so a government accreditation and review scheme is an incredibly pertinent investment—an Ofsted for avoiding catastrophic nuclear disasters. This is already partially implemented in the NCSC's Cyber Essentials evaluation scheme, with the Accreditation Bodies (AB) system allowing them to delegate the responsibility 'to carry out Cyber Essentials evaluations and certify organisations which comply with the requirements of the scheme' [12] to other businesses in order to avoid becoming overwhelmed. It will be vital, going forward, to

ensure that the certification for this scheme remains up-to-date and robust, and a balance is struck between delegating enough ABs to help with workload and not diluting the scheme.

The government also has cause to promote the creation and adoption of standards for emergent technologies, and with as much security provision baked in as possible. The previously-mentioned pervasive insecurity present across new Internet of Things (IoT) devices (for which no workable standards currently exist) may seem like a minor—practically benign—issue in isolation, for example. However, in 2016 the Mirai botnet leveraged the power of vast numbers of insecure IoT devices (including, ironically, many CCTV cameras) to perform the largest Distributed Denial of Service (DDoS) attack in history. [13] It's most disconcerting target was Dyn, which is a major player in running the Internet's DNS system—in short, the mapping system that allows Internet users to type in 'twitter.com' and be taken to the website at IP address '104.244.42.65'. [14] The thirteen DNS root servers, which serve up the Internet to all users across the globe, routinely come under DDoS attack. [15] With this massive increase in the threat from such attacks, it is likely only a matter of time before the global DNS infrastructure suffers a more serious attack, all because of insecure smart fridges. In this way, the danger of neglecting to secure systems that may seem little deserving of the effort is demonstrated.

In our modern, globally-connected world there too comes the issue of just who it is that providing one's CI services. A 2013 Intelligence and Security Committee publication claims that '[t]here is, potentially, a conflict between the commercial imperative and national security, as a result of increasing private ownership of CNI assets[...]' [16] before going on to focus on the telecommunications partnership between BT and Chinese firm Huawei, the latter accused of having links to the Chinese government that may be considered incompatible with its deep integration within the telecommunications network of the UK. These interlinkings of the joint tendrils of government and private enterprise are, throughout the world, unknowably complex—any accreditation scheme must vet potential providers with the utmost diligence.

But the major factor in business readiness for cyber security is education. A 2003 report suggested that 90% of workers would give up their passwords for a free pen. [17] The most common passwords to turn up in breaches are, year on year, the same few suspects: 'password', '123456' and 'qwerty', amongst others. [18] One of the NCSC's main aims is to improve this level of education through the issuing of '[e]xpert, trusted, and independent guidance for UK industry, government departments, the critical national infrastructure and private SMEs'. [19] This includes publishing guides for business on topics such as ransomware protection measures [20], in a similar way to the US Department of Homeland Security's Ready.gov platform. [21] Government, with its unparalleled access to global information and nationwide reach, is uniquely positioned to deliver this much-needed education.

However, any effort at education will fall short if the target audience 'don't know what they don't know'. There is a pervasive lack of awareness amongst less technical people of the dangers and pitfalls of introducing ICT into areas where it is not present, which tends to manifest in an assumption that computer systems 'just work' and an ensuing complacency. In reality, writing code is hard. It is estimated that an average of 'about 15–50 errors [are introduced] per 1000 lines of delivered code'. [22] For reference:

- Windows XP consisted of 40 million lines,
- Windows 7 consists of 50 million and
- Google is over 2 *billion*.

With the level of complexity needed in some of the systems that make up CI, it is clear that bugs and vulnerabilities are unavoidable. This needs to be common knowledge, lest the managers in charge of these CI projects fail to even look for the education and training government offers due to not understanding the risks of overestimating their own abilities—cf. the Dunning–Kruger

effect. [23]

This education cannot be limited only to technical risks either—an understanding of organisational risks and the risks inherent to any part of the system in which people are present is crucial. For the former, the importance of proper access controls must be emphasised. This means, in short, that any given operator has access only to the functionality and data that he needs and no more. This greatly mitigates the risk that a single compromised actor, or indeed a vengeful one, [24] can pose to the CI system as a whole. As for limiting the risk of those actors being compromised in the first place, comprehensive counter-social engineering training will be vital—without it, all the security in the world will be invalidated because a maintenance worker was tricked into handing his login credentials over to a web page he believed to be his bank. These attacks, known as 'phishing attacks', are a huge proportion of the attacks that will assail any system or business—they were estimated to comprise 91 % of all attacks in 2012, [25] and the cost to the UK economy year on year is enormous.

Hopefully these points demonstrate the threat posed to CI system security by human actors, and the need for any training and education programmes implemented to be aimed at *all* levels of the businesses that provide the CI in question, from the top-level managers to the lowest-level employees. All are potential threat vectors (even the director of the CIA couldn't be trusted [26]). Crucially, these must also be solutions designed to deliver results over the long term—one author writes in *The Economist* that '[u]nfortunately, there is a mismatch between political attention spans and infrastructure investment timeframes[...]', [27] but this short-sighted laxity cannot be tolerated in an area with as much inherent risk as CI security. Cross-bench politicking is the solution to this; schemes put in place cannot be left at the risk of harm in the event of a given party's loss of government.

4 Conclusion

The running of a nation requires a base level of guaranteed service provision from the various forms of national infrastructure. As these services move to increased automation and cyber integration in order to boost output and efficiency, they open the nation up to many new possibilities of attack. There are also inconceivably complex levels of inter-connexion between these services, so that failure in one can lead to a cascade of failures in others. Anecdotally, shortly after the 9/11 attacks many buildings across New York City had to be evacuated—not due to any damage to the structures themselves, but rather the lack of a water supply caused by ruptured water mains elsewhere.

Whilst the running of many of these services is left to private industry, the responsibility for security cannot be so delegated—a catastrophic breach in the critical national infrastructure will be more damaging for the nation which depends on it (and the government which governs the nation) than the likely multinational business in charge at the time.

Alongside this, government is uniquely positioned to deliver intelligence and education to the sector to a high level. Why is doing so so vital an effort? An unnamed NSA operative's testimony, as featured in *Zero Days*, puts it best: '[W]hen you shut down a country's power grid, it doesn't just pop back up. It's more like Humpty-Dumpty. And if all the king's men can't turn the lights back on—or filter the water for weeks—then lots of people die.' [10]

REFERENCES

[1] [Online]. Available: https://www.cpni.gov.uk/critical-national-infrastructure-0

[2] W. Ashford, "Is uk critical national infrastructure properly protected?" 2011. [Online]. Available: http://www.computerweekly.com/news/1280097313/Is-UK-critical-national-infrastructure-properly-protected

[3] *Presidential Decision Directive/NSC-63*, 1998.

[4] *National Security Strategy and Strategic Defence and Security Review 2015*, 2015. [Online]. Available: https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015

[5] *National Cyber Security Strategy 2016–2021*, 2016. [Online]. Available: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[6] 2017. [Online]. Available: https://www.ncsc.gov.uk/about-us

[7] R. Langner, *Cracking Stuxnet, a 21st-century cyber weapon*, 2011. [Online]. Available: https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon#t-534190

[8] K. Zetter, "Inside the cunning, unprecedented hack of ukraine's power grid," 2017. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[9] J. Leyden, "Ddosing has evolved in the vacuum left by iot's total absence of security," 2017. [Online]. Available: https://www.theregister.co.uk/2017/01/24/ddos_sitrep/

[10] Alex Gibney, 2016.

[11] S. Pritchard, "Cyber attacks on national targets grow," 2014. [Online]. Available: https://www.ft.com/content/d71fe198-c3cc-11e3-a8e0-00144feabdc0

[12] *Cyber Essentials Accreditation Bodies*, 2015.

[13] 2016. [Online]. Available: https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html

[14] K. York, "Dyn statement on 10/21/2016 ddos attack," 2016. [Online]. Available: https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

[15] [Online]. Available: https://en.wikipedia.org/wiki/Distributed_denial-of-service_attacks_on_root_nameservers

[16] *Foreign involvement in the Critical National Infrastructure: The implications for national security*, 2013. [Online]. Available: https://www.gov.uk/government/publications/foreign-involvement-in-the-critical-national-infrastructure-intelligence-and-security-committee-report

[17] J. Leyden, "Office workers give away passwords for a cheap pen," 2003. [Online]. Available: http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/

[18] C. McGoogan, "The world's most common passwords revealed: Are you using them?" 2017. [Online]. Available: http://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/

[19] [Online]. Available: https://www.ncsc.gov.uk/guidance

[20] 2016. [Online]. Available: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

[21] [Online]. Available: https://www.ready.gov/cyber-incident

[22] S. McConnell, *Code complete*. Pearson Education, 2004.

[23] J. Kruger and D. Dunning, "Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments." *Journal of personality and social psychology*, vol. 77, no. 6, p. 1121, 1999.

[24] K. McCarthy, "I was authorized to trash my employer's network, sysadmin tells court," 2017. [Online]. Available: https://www.theregister.co.uk/2017/02/23/michael_thomas_appeals_conviction/

[25] D. Stephenson, "Spear phishing: Who's getting caught?" 2013. [Online]. Available: https://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught/

[26] M. Apuzzo, "Petraeus reaches plea deal over giving classified data to his lover," 2015. [Online]. Available: http://www.nytimes.com/2015/03/04/us/petraeus-plea-deal-over-giving-classified-data-to-lover.html

[27] G. Cohen, "Financing the uks infrastructure: private and public gains," 2016. [Online]. Available: https://www.eiuperspectives.economist.com/economic-development/vibrant-economy/blog/financing-uk%E2%80%99s-infrastructure-private-and-public-gains