Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat

Adam Henschke

Abstract In this chapter I present an argument that cyber-terrorism will happen. This argument is premised on the development of a cluster of related technologies that create a direct causal link between the informational realm of cyberspace and the physical realm. These cyber-enabled physical systems fit under the umbrella of the 'Internet of Things' (IoT). While this informational/physical connection is a vitally important part of the claim, a more nuanced analysis reveals five further features are central to the IoT enabling cyber-terrorism. These features are that the IoT is radically *insecure*, that the components of the IoT are *in the world*, that the sheer numbers of IoT devices mean potential attacks can be *intense*, that the IoT will likely be powered by a range of Artificial Intelligence aspects, making it *inscrutable*, and that the IoT is largely *invisible*. Combining these five factors together, the IoT emerges as a threat vector for cyber-terrorism. The point of the chapter is to go beyond recognising that the IoT is a thing in the world and so can enable physical impacts from cyber-attacks, to offer these five factors to say something more specific about just why the IoT can potentially be used for cyber-terrorism. Having outlined how the IoT can be used for cyber-terrorism, I attend to the question of whether such actions are actually terrorism or not. Ultimately, I argue, as the IoT grows in scope and penetration of our physical worlds and behaviours, it means that cyber-terrorism is not a question of if, but when. This, I suggest, has significant ethical implications as these five features of the IoT mean that we ought to be regulating these technologies.

1 Cyber Terrorism Has Not Taken Place

In 2013 Thomas Rid published his book *Cyberwar Will Not Take Place* [48]. It has been the topic of considerable attention, with many people offering criticisms on a range of points that he makes [4]. However, despite a world that is facing increasing instability in its geopolitics, and as a range of high-profile information operations

A. Henschke (✉)
Philosophy Section, University of Twente, Enschede, The Netherlands
e-mail: a.henschke@utwente.nl

A. Henschke et al. (eds.), *Counter-Terrorism, Ethics and Technology*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-90221-6_5

show the centrality of cyberspace to national security, Rid's titular premise has held out—nothing in the cyber realm has met the criteria to make it an act of war. Stuxnet is instructive here. More than ten years after the event, Stuxnet is still one of the most high-profile cyber-attacks due to it being proof of concept that cyber-attacks can cause physical impacts. Yet, in line with Rid's point, Stuxnet is important because of its uniqueness. There is yet to be another cyber-attack that brings about physical impacts, or at least, one that is publicly known. And definitely nothing that rises to a level that would classify as armed attack. So, despite Rid's arguments facing criticism, his conclusion seems to be holding out.

Looking at terrorist use of the internet, despite their highly sophisticated use of the internet for recruitment, radicalisation, and propaganda [5], even the so-called Islamic State (IS) at their peak did not manage to engage in cyber-terrorism *proper*, see following for what that means. As Julian Droogan and Lise Waldek point out, "in the realms of academia, policy and the media [have] provided many foreboding and even doomsday warnings about the future of cyber-terrorism, which in the main have failed to come to realization" [16]. So-called IS used cyberspace to motivate and guide a range of terrorist acts [5], and as counter-terrorism actors stepped up their actions—including actions in cyberspace—to disrupt larger high profile terrorist activities around the world [7], so-called IS evolved their strategies [29–31] to encourage low technology small group acts of terrorism, using whatever technologies they had at hand—as a spokesperson for so-called IS stated in 2014, "If you are not able to find an IED or a bullet, then single out the disbelieving American, Frenchman, or any of their allies. Smash his head with a rock, or slaughter him with a knife, or run him over with your car, or throw him down from a high place, or choke him, or poison him" [44]. Yet, despite their evolution toward small scale ongoing acts of domestic terrorism, even so-called IS did not mount any successful cyber-terrorism acts. To be clear, so-called IS did use the internet for cyber-attacks [2]. However, insofar as terrorism necessarily involves physical violence, or the credible threat of physical violence, they did not engage in cyber-terrorism.

This turns us to a definition of cyber-terrorism. Terrorism is a complex action that relies on two targets of attack [12, 46]. First is the attack itself. In most accounts of terrorism, the terrorist action uses physical violence to attack people [46] or perhaps their property [12]. The second target is political and social leaders and wider community. It is not simply "the organized use of violence to attack non-combatants ('innocents' in a special sense) or their property" but organized violence "for political purposes" ([12], 5). The intent of the terrorist attack is not violence for the sake of violence but that in response to this attack, people's behaviour changes. Ideally, the targeted people and/or their political representatives change some law, policy, practice or behaviour in line with the terrorist's ends.

The issue here is that, to date, terrorist use of the internet has not included efforts where the internet has been used *directly* to bring about *physical violence*. This a vital distinction—if we understand cyber-terrorism to be simply about use of the internet to spread fear or bring about political changes, then we are talking about propaganda or information operations. And while these are important issues, and play a big role in modern international terrorism, I suggest that this is not cyber-terrorism. Contrast

a message posted online that says "we are going to harm you", with a terrorist action that involved hijacking autonomous vehicles and using the hacked vehicles in coordinated vehicular attacks against pedestrians. Subsequent to the attack, the terrorists broadcast a message that says "we were behind these attacks. And if you don't follow our demands, we will continue to harm you." The first example was merely the use of the internet to communicate a threat. The second is the use of the internet to bring about physical violence, coupled with a larger socio-political agenda. While we have seen many instances of the first example, to date we have not seen any instances of the second.

The reason that neither cyber war nor cyber-terrorism have happened, is due in part to the limited capacity for cyberspace to have direct causal impacts in the physical world. The core of Rid's argument turns out to be true in the world. "[M]ost cyber-attacks are not violent and cannot sensibly be understood as a form of violent action" [13, 48]. The original 'Tallinn Manual' holds such a view, exemplified by its Rule 11: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" [52]. Something like Stuxnet is an aberration; very few cyber-attacks do have the direct impact on the physical realm to count as physically violent. And, in line with the Tallinn Manual's reasoning, no cyber-attacks have risen to a level comparable to that of physical use of force that would constitute a 'just cause' for war. So, descriptively, cyber-attacks simply have not had the physical impacts to be considered war or terrorism. In line with the definition above, I am using cyber-terrorism here to mean something like the use or exploitation of the internet to bring about an act of physical violence directed against non-combatants or innocents, to achieve some secondary ideological, religious or political purpose. Importantly, as will be discussed toward the end of this paper, these acts have to be high profile; they need wide coverage or publicity to ultimately be considered successful. Thus in this description, neither so-called IS nor any other modern terrorist group has used cyberspace to engaged in acts of physical violence to achieve these secondary ends.

However, this is not a permanent fact about cyber-attacks. Looking closer at Rid's reasoning will help explain why. "Code doesn't have its own force or energy. Instead, any cyber-attack… has to utilize the force or energy that is embedded in the targeted system or created by it…Computer code can only directly affect computer-controlled machines, not humans" [13, 48]. On Rid's account, something like a malicious computer virus is something composed of computer code and can only act upon other computer code. A computer virus is importantly different from a biological virus [48, 13–14]. The biological virus directly impacts the host's body, while the computer virus can only impact other code. According to Rid, code can only act on code.

For the purpose of this chapter, I am accepting Rid's narrow claim about code-on-code being the only way to conceptualise cyber-attacks and his position that violence is only physical. There is an interesting discussion about narrow/wide definitions of violence,[1] and that if we have a wider view of violence we might rethink what counts

[1] For more on different ways conceive of violence see: [13, 15, 19].

as terrorism. Jessica Wolfendale's chapter in this book touches on some of those issues. My point is that even if we accept Rid's narrow account about cyber-attacks being code-on-code, and a narrow definition of terrorism that is limited to acts of, or credible threats of, physical violence, the IoT makes cyber-terrorism a meaningful term.

The reason is that the IoT is a cyber-physical system,[2] and so has the capacity for code to have 'direct' physical causality. Many elements of the IoT forge a direct link between code and actuators [3]. Actuators are elements which, upon receiving a code-driven command, will bring about some physical change in the world. Think here of a smart car that has remotely activated door locks. Communications between the car owner's mobile phone and the car mean that the doors will be unlocked as the owner approaches the car. Due to commands from code, the locks move. The code is causing changes in the physical world. Contra Rid, the informational realm is no longer simply code-on-code, it is code-to-world. The IoT exists across, and actively seeks to link the information with the world, the cyber realm and physical realm now have a direct causal connection. As I have argued elsewhere, this combination of cyber and physical realms means we need to consider both in any assessment of the IoT [26]. Moreover, this relation is dyadically causal[3]—the cyber realm influences the physical and the physical influences the information. So, the IoT means that one of Rid's key premises, that code only acts on code, is no longer correct.

2 The IoT: Cyber-Physical Systems That Will Span The Globe

Before going further, we need to clarify what is being referred to when discussing the IoT. In short, this can mean any device or thing in the world that is 'smart' and connected with other devices. "'The IoT' is a broad, and deliberately vague catch all term to describe a range of integrated technology types that include (1) sensors, 'things that gather information', (2) communicators, 'things that communicate information' (3) actuators, 'things that change the physical world' and (4) AI, things that process information [3, 55–56]. The IoT can include individual devices or components, like a smart TV, a small networked set of devices like a smart home or a large complex system of devices like an autonomous driving system.

[2] Groups like the United States National Science Foundation use the term 'cyber-physical system'. "Cyber-physical systems (CPSs) are transforming the way people interact with engineered systems, just as the Internet transformed the way people interact with information. CPS integrate cyber components (namely, sensing, computation, control, and networking) into physical components (namely, physical objects, infrastructure, and human users), connecting them to the internet and each other" [18, 53, xxix].

[3] A dyadic relation is one that recognises "the idea of mutual causation. There is a particular 'whole' which consists in two elements, each of which stands in a causal relation to the other" [25, 267]. For more on this idea of dyadic relations, see [25, 170–173].

The changes brought about by the IoT that make it relevant for a discussion of cyber-terrorism. The IoT enables the informational realm and the physical realm to be causally connected. This occurs is through the use of actuators. Actuators are components which allow information, or code, to be translated into changes or impacts in the physical world. It is these actuators that allow information to make these systems cyber-enabled *physical* systems. In addition to the issues of physical safety arising from these actuators, this physicality of the IoT marks it as importantly distinct from the internet. The internet, as we typically understand it, is primarily an informational network. While it exists in, and relies on things in the physical world [33], it is largely constrained to cyberspace. Rid's argument is that because cyber-attacks are code-on-code, their impacts are primarily contained to the cyber realm [48]. The IoT breaks this division. Due to the causal connection between code and actuators, code can now bring about physical impacts.

Moreover, the IoT is expected to be immense. Current estimates "project that there will be more than 41 billion IoT devices by 2027, up from about 8 billion in 2019" [43]. This leads some to predict an investment of 1.7 trillion U.S. dollars by 2020 [32]. The annual investment is now predicted to be $2.4 trillion by 2027 [43]. Its scale alone will mean that it will bring immense change to our lives. Moreover, the IoT will likely reach into all facets of our lives, the personal in the form of smart homes, the professional in the ways that it will guide working life, the system in how it will affect things like logistics, even the governmental and military.

So, putting these aspects together, we have a scenario where the informational realm and the physical realm are now directly interacting with each other, that may cover the globe and penetrate our personal, professional, social and political lives. Contra Rid, cyberspace is no longer just code-to-code. These elements, I suggest, present terrorists with a capacity to use the internet to cause significant physical violence in order to bring about ideological, religious or political changes. As such, I suggest that cyber-terrorism will take place.

3 So What? An Inventory of Features

This chapter could stop at that, but a more nuanced analysis will give us a greater understanding of the particular vulnerabilities of the IoT that make it an ideal novel means for terrorist attacks. In this section, I present an inventory of features that clarify the point that cyber-terrorism will happen. I argue that

(1) the IoT is radically *insecure*,
(2) that components of the IoT are *in the world*,
(3) that the sheer numbers of IoT devices mean potential attacks can be *intense*,
(4) that the IoT's reliance on AI present further challenges arising from the *inscrutability* of AI, and
(5) that the IoT is largely *invisible*.

And, in combination, this inventory of features makes the IoT a way for cyber-terrorism to happen.

The IoT is widely acknowledged to be radically *insecure*. This insecurity has led people to describe it as the 'internet of insecure things' [10] and 'the internet of threats' [41]. In one example of how this insecurity can lead to significant personal risk, one woman was stalked by an ex-partner, who through "simple technology and smartphone apps that allowed him to remotely stop and start her car, control the vehicle's windows and track her constantly" [54]. A widespread IoT that is integrated into our lives will be like this but many times more powerful and pervasive.

This radical insecurity is brought about by a combination of two aspects of the IoT. As mention above, the IoT is composed of things that are in communication with each other. Not only do many IoT devices have sensors gathering information on the world around them, that information is then communicated. Thus, there will be a wealth of information being shared *between* a range of interconnected components and devices. In an insecure system, that personal information can potentially be accessed by people without the user's consent. We have seen examples of this with 'smart toys', children's toys with remotely accessible cameras and other sensors present significant security vulnerabilities [11, 24]. A number of smart technology companies have either been shown to be, or publicly admitted to, using cameras and microphones in smart televisions [39, 51]. Devices like Google Home and Amazon's Alexa [1, 55] allow for remote surveillance in the home. And in perhaps the creepiest example, We-Vibe, a company that produces smart internet connected sex toys, was shown to be gathering user data [47]. We-Vibe were gathering information about how their sex toys were used, the duration and intensity of use, even the temperature of users was gathered and sent back to the company without user knowledge or consent.

This brings us to the radically insecure aspect of the IoT. We-Vibe's misuse of personal information became apparent when their product was hacked by a group of 'white hat hackers'.[4] The security on the We-Vibe product was limited at best. This radical insecurity is seen to be pervasive across many IoT devices and products [10, 41]. The basic cyber-security on these things is relatively weak. Second, the passwords that they do have are typically and frequently set to a factory default and then not changed or complex for users to change.

The limited security serves a range of purposes. It makes it easier to install and use the IoT devices. In the ideal scenario, a user buys a device, takes it home, to the office, etc., activates and it merges seamlessly with the communications networks and other relevant devices [9, 14]. However, if one was to have complex security protocols that needed to be run prior to the device coming into operation, this would not only be more time consuming for the user, it would increase the likelihood of connection problems. As anyone who has tried and failed to get Bluetooth devices to pair with each other can attest, connection problems with smart devices can be incredibly frustrating and time consuming. If the connection is not successful, it can either defeat the purpose of purchasing the device and may even render the device

[4] White hat hackers are people who hack into devices or information systems to alert owners, users and manufacturers to security vulnerabilities and failings [38].

useless. Further, the limited security keeps costs down. So, ease of use, efficacy of use and costs are values that drive design and security defaults toward lower security features.[5]

Adding to this, malicious agents can access information about factory default passwords online, and so gain access to the information gathered and communicated by the devices. Shodan, for instance, "is a search engine for exploring the Internet and thus finding connected devices. Its main use is to provide a tool for cybersecurity researchers and developers to detect vulnerable Internet-connected devices without scanning them directly" [17]. While this insecurity alone does not necessarily mean that an IoT device could be weaponised by terrorists, the radical insecurity is part of a set of features that make the IoT an ideal target for tech savvy terrorists. Think here of an autonomous vehicle with weak security—should a terrorist discover that this security vulnerability allows for remote control of steering, breaking or accelerating features, the car becomes part of a terrorist attack. And if a series of attacks occurred, not only would that likely cause significant damage to trust in autonomous vehicle systems [27] it could neatly fit with certain terrorist's second order aims, a point I return to at the end of this chapter.

The second feature of the IoT that makes it a potential target is that these devices are *in the world*. We have already touched on the way that the code-to-world aspect of the IoT means that it could allow for terrorists to bring about physical violence. This is because the IoT is not constrained to the informational realm. It is in the world, and so—depending on the particular devices—can allow for a cyber-attack to bring about physical violence. Think again of an autonomous vehicle being taken over by terrorists. The deliberate use of cars and trucks in terrorist attacks around the world [42] show how vehicles are an increasing weapon of choice for terrorists. With autonomous vehicles this could be done remotely. Of course, autonomous vehicles with such security flaws would likely not be allowed on the road. My point here is that the elements of IoT components that are in the world means that certain IoT devices, like cars, can potentially be used for physical violence.

We can also think about the security challenges posed by the IoT being in world in a different way. Think here that IoT users are primarily civilians, non-combatants or non-security actors. This means that those users are likely not going to have concerns about terrorists using the IoT against them. However, the familiarity with IoT devices can breed lax security practices. For instance, consider security sector actors, like those in military, intelligence, diplomatic or policing roles using IoT devices with a civilian mindset. The point here is that in a world of 'bring your own device', those from the security sector need to be extra careful with IoT devices. Consider here the example of the Strava fitness tracking app. Strava was an IoT device in which people's exercise habits were monitored and shared to publicly accessible social media. A junior university researcher was interested in this publicly accessible information and used it to identify US military and spy bases.

> Strava, a fitness-tracking app, is revealing potentially sensitive information about military bases and supply routes via its global heatmap website. The data map shows 1 billion activities

[5] I have argued this point in more detail in the design of autonomous vehicles.

> and 3 trillion points of latitude and longitude from "Strava's global network of athletes", according to the American company. On the weekend, 20-year-old Australian university student Nathan Ruser noticed the map showed the locations and running routines of military personnel at bases in the Middle East and other conflict zones… While security analysts often use satellite imagery to study military installations, Mr Ruser said the Strava data added an additional, possibly dangerous layer of information. Using satellite imagery, you can see base buildings, for example. But on the heatmap, you can see which buildings are most used, or the jogging routes of soldiers [8].

The point here is twofold. First, IoT devices can provide security sensitive information if user behaviour considers these devices with a civilian mindset. That is, because we are familiar with them in a non-security context, we can easily overlook the security threats that they pose. Second, as these devices are in the world, upon analysis they can provide interested parties with useful information about user habits in the world. This derived information can then pose security risks. Whether it is habits of security personnel on military bases, or more general civilian habits like driving patterns, such information derived from the physical presence of these devices can be very useful to terrorists and other malicious actors. I have written elsewhere how the collection, aggregation and analysis of innocuous information can reveal virtual identities of people [25]. The IoT will only add to this capacity to gain increasingly revealing and powerful information about people, which then has significant security implications.

This alone would not seem too relevant to cyber-terrorism. However, when you combine the radical insecurity with the fact that there are billions of IoT devices in the world, you have the potential for *intense activity*. The point here is that malicious actors like terrorists can exploit IoT's numbers for cyber-attacks. Consider that there have been cyber-attacks that have used 'smart devices' like smart fridges with poor security for DDOS attacks [37]. As mentioned, by 2027 some estimate that there will be more than 40 billion IoT devices in the world [43]. The sheer numbers of IoT devices mean that it can act as a force multiplier. As the DDOS examples show, the IoT can be harnessed for other cyber-attacks. Similarly, the number of IoT devices mean that the effects of an IoT attack can potentially be disastrous. Consider here if a smart house has an unsecured IoT enabled heater. If an attacker was to take over this heater, they could turn the temperature of the house up remotely, which is obviously of minimal concern. However, if this attack took over hundreds of thousands of these heaters during a heat wave, it could bring down regional power supply, potentially increasing the number of vulnerable people like the elderly that can die during the heat wave. Thus, the sheer number of IoT devices in the world mean that critical infrastructure is vulnerable to cyber-attacks.[6]

The point here is that, not only does the IoT allow for code to impact the physical realm, but the sheer number of IoT enabled devices in the physical world mean that physical things can have significant impacts at a higher level than what a pre-IoT cyber-attack could cause; the number of devices vulnerable to attack means that

[6] Note that on the definition of cyber-terrorism above, such cyber-attacks would not yet constitute cyber-terrorism. The exploitation of the IoT for physical violence needs to be in service of some secondary ideological, religious or political purpose.

these attacks can be intense. The number of these devices in the world, coupled with their radical insecurity mean that a malicious actor can use the IoT to bring about significant disruption in the cyber realm and that this can then have physical impacts. While this is might still be code-to-code attacks in a narrow sense, it is enabled by the numbers of IoT devices in the world.

AI is likely to be an increasingly important part of the IoT. This is because there will be so many connected devices in the IoT. "To reap the actual benefit of IoT, it has to be intelligent" [45, 1]. Given the sheer numbers of IoT devices, there will be a cluster of parallel IoT systems that require co-ordination. Whether it is the devices in one IoT system, or the integration of different systems, the only way that the more complex IoT systems and integrated systems will be able to operate seamlessly, at speed, without human interaction is through AI [21]. In addition, the vast amounts of information that will be gathered and communicated by these devices will dwarf what the internet is currently producing: One current estimate suggests that IoT devices generate 1 billion GB of data each day [21]. Again, the only way that this can be managed is through AI. The problem with AI is that it can be *inscrutable*.[7]

This, inscrutability I suggest, presents an ideal point of vulnerability for terrorists to exploit. Trust is essential for autonomous vehicle systems to function effectively [27], and I suspect that this claim will hold for many IoT systems. If people do not trust the system, they are either not going to use it, or will not use it to its full effect. However, given the inscrutability of the system, it might be impossible to prove that the decision support systems provided by the AI are safe or reliable. The inscrutability of the AI allows for terrorists to exploit confusion and sew mistrust. On its own, inscrutability is not a major terrorist risk, but couple the AI with the IoT being in the world, allowing for intense activity and its radical insecurity and you have a viable threat vector for terrorist activity.

The final feature that means the IoT is a viable threat vector for cyber-terrorism is that it is *invisible*. This invisibility occurs in a range of layers. The actual components of the IoT are going to be typically invisible—cameras in televisions, microphones in smart watches, locks in car doors. A key technological development enabling the IoT is the miniaturization of its components.[8] The sensors, the communicators, the actuators, these technological components that enable the IoT are all undergoing rapid and substantive miniaturization, allowing them to be integrated into a range of different applications [23, 34]. They can be potentially everywhere in our physical world, and by design, we will literally overlook them. When working as it should, the user should be unaware of the IoT devices and components.

---

[7] Note here that I am agnostic about whether the components of the IoT will be automated or have some form of autonomy. Likewise, I am agnostic whether these systems are just information handling devices or if they come closer to proper intelligent systems. The point of this section remains the same. Nothing for my point relies on the IoT systems being properly autonomous, intelligent, sentient, having moral agency and so on.

[8] For instance, "[r]ecent advancement of miniaturization in manufacturing allows IoT devices to easily be loaded into unmanned drones and vehicles because of miniaturized sizes and light-weight designs" [34, 102]. This miniaturization of sensing devices is predicted to play an increasingly important role in the application of the IoT to healthcare [23, 40].

Further, the people in the IoT are invisible. The invisibility of people in the IoT occurs in a complex interactive set of ways. Remote users can be invisible to other users. The designers, and the choices that they have made in the design and decision features of the IoT's components, are typically invisible to most users. Those people who inhabit roles in the oversight mechanisms are likely to be invisible to users. In a poorly designed systems, the users themselves can often be invisible to designers and oversight bodies.[9] This occurs in part when there are poorly designed features that do not take people into account—an autonomous vehicle that allows for a car to be remotely hacked by a malicious actor for instance has not taken into account the threat posed by some people. In addition, users are often invisible to designers in that it is hard to predict how people will actually use, misuse or hack a piece of technology. Moreover, the complexity of ways that a set of people, using technologies in the real world, in cooperation and competition with each other, makes it very hard if not impossible to predict, design and write laws for every possible combination of use.

Finally, the risks are invisible. While the insecurity, the IoT being in the world, the potential intensity of cyber-attacks and inscrutability alone do not alone necessarily make the IoT a means for cyber-terrorism, *in combination they do.* This is essentially an 'emergent risk'. By this I mean that the combination of these features presents a novel system-level risk that can only be properly understood when looking at the combination of these factors. The combination of the IoT being radically insecure, in the world, intense, and inscrutable is a system level phenomenon that can only be properly explained when seen from the system level. This notion is explained by reference emergence. "Emergence is said to occur when certain properties appear in a system that are novel or unexpected and go beyond the properties of the parts of that system" [35, 277]. We lose explanatory power if we look only at each factor independently. By suggesting that we see the IoT as presenting an emergent risk, we are able to better recognise and understand how it can be used for cyber-terrorism. That is, in combination, we have made the risk visible.

4 Will IoT Enabled Cyber-Attacks Be Acts of Terrorism?

I have presented a case that five aspects of the IoT in combination present, not just a risk but, a *terrorist* risk. There are, however, two counter-arguments to engage with before we accept the claim that cyber-terrorism will happen. First, is whether an IoT enabled attack counts as terrorism. Second is whether an IoT enabled act of cyber-terrorism is likely.

For the first counter-argument we return to Rid's scepticism about cyber-attacks being violent. Recall that on Rid's view, a cyber-attack was code acting on code, so

[9] In their overview of value sensitive design (VSD), Batya Friedman and David Hendry discuss in great detail the need for effective and ethical design to take in the views, needs, values and practices of a large range of stakeholders, including but not limited to direct and indirect users [20, 35–44].

not physical and therefore not violent. As we have discussed, however, the IoT is a complex set of cyber-enabled physical systems. People are physically vulnerable to the IoT in ways that we are not physically vulnerable to the internet. The five features of the IoT listed above: it is insecure, in the world, intense, inscrutable, and invisible mean that we can reject a position like Rid's—an unsecured set of IoT devices that pose physical risks to people can allow code to act in the world.

However, there is a second aspect to the IoT that perhaps should give us pause to consider an IoT attack, even if it is in the world, is it an act of *terrorism*? While it is plausible to suggest that many IoT enabled acts of terrorism might be limited to physical property and not people, the physical nature of the IoT means that a well thought out terrorist attack puts people at physical risk.[10] The most obvious scenario is that a group is inspired by the way that so-called IS and right wing extremists have started using cars to deliberately drive into groups of people [42]. While such an attack is—arguably—an attack on physical property, the relevant factor is that that physical property is then used to physically harm people. To reiterate a point made above, autonomous vehicle designers take these risks quite seriously so it is hopefully unlikely that such an attack might occur. However, as the IoT becomes more widely dispersed and deeply integrated into our lives and world, the risk of some aspect of it being hacked to cause physical harm to people is something that should not be dismissed. Just as a set of box cutting knives enabled the hijacking of planes on 11 September, all it takes is a creative thinker to exploit some combination of factors in the IoT to engage in an act of cyber-terrorism. And as I have showed with the inventory of five features of the IoT, it presents an attractive target for terrorists. Further to this, as so-called IS showed, modern terrorism is not shy of using either modern information communications technologies or common items like cars to further their terrorist aims. The motivation is there, and the IoT provides the means for cyber-terrorism to occur.

The second counter-argument is scepticism about whether such IoT enabled cyber-terrorism is *likely* to happen. Terrorism is not simply concerned with physical violence against innocent people, but some second order effects. Again, terrorism, it is "the deliberate use of violence, or threat of its use, against innocent people, with the aim of intimidating some other people into a course of action they would not otherwise take" [46, 24]. Essential to any successful act of terrorism is that it brings about the second order political, religious or ideological ends that motivate the group. Or at very least, that the act of terrorism uses physical violence to draw attention to those political, religious or ideological ends. "The success of a terrorist operation depends almost entirely on the amount of publicity it receives…Thus in the final analysis, it is not the magnitude of the terrorist operation that counts but the

[10] We have also recently seen that a cyber-attack on a hospital caused a death resulting from disruption to the IT system: "the first known fatality related to ransomware occurred in Duesseldorf, Germany, after an attack caused IT systems to fail and a critically ill patient needing urgent admission died after she had to be taken to another city for treatment." [6]. This example, however, is an act of cyber-crime, rather than cyber-terrorism, as it lacks the secondary ideological, religious or political purpose necessary to make it an act of terrorism. But it does show how cyber-security can be a matter of life and death.

publicity; and this rule applies not only to single operations but to whole campaigns" [36, 109]. The likelihood of an IoT enabled cyber terrorist act occurring is thus a function of the anticipated publicity that the act will receive.

As Paul Gill et al. note, terrorist groups often display a capacity for "malevolent creativity" [22, 130]. One of the features driving terrorist creativity is the novelty of an attack: "Spontaneous novel acts of violence generate effective surprise within the target audience" [22, 134]. Here, one can only speculate, but the relative novelty of particular IoT systems seems like they are an ideal means of a shocking terrorist act. As these systems are new, they are particularly vulnerable to the fear that results from a terrorist attack. Consider again autonomous vehicles. "If trust is necessary for effective driving, then the background beliefs about *whether* the given technologies and systems are trustworthy will impact how and when people drive. This in turn depends on whether the drivers see other drivers, road users and the system itself as trustworthy. Moreover, once trust is lost it can be very hard to repair" [27, 89]. If an IoT system was to be the subject of a terrorist attack, then it is likely that many users and relevant oversight bodies would either cease using the system or demand significant security changes as they see the overall system as untrustworthy. While in the long term, increased security would ideally reduce the risk of ongoing cyber-terrorism, the fear that a high profile attack would generate and the reduction in use cause by a loss of trust would fit the second order aspect of terrorism. And the fact that changes would be made is evidence of the success of the attack—think here of the security response to air travel following high profile terrorist acts that targeted planes.

The likelihood of such attacks becoming widespread is likely going to be a combination of the amount of public coverage that such attacks generate, and how the publicity around the attacks connects with the larger ideological, religious or political purpose of the terrorist actors. My speculation here is that, at least in the early days of such IoT enabled cyber-terrorism, the attacks will be seen as both novel, and provide some high level of spectacle, thus attracting a lot of publicity.

5 Ethics and Responsibilities for IoT Enabled Cyber-Terrorism

To close this discussion, let us put this in the context of ethics. The chief ethical issues here are concerned with responsibility for IoT enabled cyber-terrorism. If, as I have suggested, cyber-terrorism will be enabled by the IoT, then what ought we do about it? The five features described provide us with a way to get some nuanced ascription of responsibility. First, and foremost, the radical insecurity of the IoT needs to be dealt with. This is in part a governmental responsibility—it is national governments who have the capacity to draft and enforce laws that ensure minimum security standards. However, unlike many other areas of counter-terrorism, service

and technology providers also bear some responsibility here. If security vulnerabilities in their products and services that allow for the IoT to enable cyber-terrorism, then it is incumbent upon them to resolve those security failings.

Second, that the IoT is in the world entails a responsibility on governments, technology designers and providers, and consumers to be aware of the risks that their IoT components pose. The point here is that if the products and services that we use in the world provide the infrastructure for cyber-terrorism, then we all have a responsibility to do what we can to mitigate this risk. This would include things like ensuring that our own IoT devices have their security updated and upgraded as necessary. Importantly, such resolutions to the issues of security are not going to happen without recognition of the risks posed by these things in the world.

Third, on the issue of intensity, following the responsibilities for insecurity and the IoT being in the world, if we take the vulnerabilities posed by the IoT seriously, then we should hopefully have significantly reduced the potential for intensity of the cyber-attacks. The responsibility here falls again on governments, technology designers and providers, and consumers.[11]

The inscrutability of AI and its potential role in cyber-terrorism presents a very novel challenge. However, there is a burgeoning literature on the ethical importance of explicability that we can draw from here. "It is rare to see large numbers of ethicists, practitioners, journalists, and policy-makers agree on something that should guide the development of a technology. Yet, with the principle requiring that [AI] be explicable, we have exactly that. Microsoft, Google, the World Economic Forum, the draft AI ethics guidelines for the EU commission, etc. all include a principle for AI that falls under the umbrella of 'explicability'" [49, 498]. My suggestion here is that explicability, the process by which we reduce inscrutability, needs to be pinned to two parallel principles. When an act of cyber-terrorism appears to have used the IoT we need some processes that can *ensure* that such vulnerabilities are identified and mitigated, and that we can *assure* the public at large that these vulnerabilities are in fact being dealt with.[12] Again, by identifying the feature of inscrutability in IoT enabled cyber-terrorism, we need to find some way of assigning responsibility to governments for oversight, to technology designers and producers to ensure that their products are robust, that can take into account the public facing aspects of the IoT, and its relation to cyber-terrorism.

Finally, to the invisibility of the IoT, we find a further aspect that helps clarify ethical responsibility for such cyber-terrorism. As argued, there are a series of ways that the IoT is invisible to people. The point here is that we generally hold that a person is not to be held responsible for something that they are ignorant of. For instance, if it was my autonomous vehicle that was hacked and used in a terrorist attack, but I was not to know that it presented such a risk, to paraphrase Michael Zimmerman,

[11] See also the chapter by Alastair Reed and Adam in this collection for more on this discussion of the responsibility of technology companies around modern terrorism.

[12] In a co-authored article, I have argued elsewhere about the need for ensurance and assurance mechanisms with surveillance technologies in liberal democracies, and many of the points there hold here [50].

most would say (and I would again be inclined to agree) that I am not to blame for an act of IoT enabled cyber-terrorism, unless I am to blame for my ignorance.[13] This relation between knowledge, ignorance, and responsibilities is a controversial and contested area. As Zimmerman suggests, we must factor in whether a person is to be blamed for their ignorance, "to say that Perry ought to have known better is to imply that he could have known better-he was free to know better" [57, 413].

However, we can suggest some rules of thumb here—we ought not hold consumers and IoT users responsible for IoT enabled cyber-terrorism if they were reasonably ignorant of the way that their IoT components could be utilised in an act of cyber-terrorism. Given their knowledge of the products and their likely uses, designers and technology producers, however, would have to justify why they were justifiably ignorant that their particular design and products could be used for cyber-terrorism. That is, when thinking of consumers and users, the burden of proof is generally on those seeking to show why the consumer and user ought to be held responsible, while when considering designers and producers, the burden of proof is generally going to be on them to justify why they ought not be held responsible. While each particular instance requires nuance and detail, the rules of thumb are usefully derived from recognition of the invisibility of the IoT. Again, the five features of the IoT give us a way to at least start a nuanced conversation about the ascription of responsibility.

To conclude, in this chapter I mounted an argument that the IoT will enable cyber-terrorism. Given that the IoT is a cyber-physical system, we can reject a Rid style claim that cyber-attacks are only code on code. The causal links between sensors, communicators and actuators mean that a code-based attack can have physical effects. Moreover, I have listed an inventory of five further features that make the IoT a threat vector for terrorism. I showed that the IoT lacks significant security protections making it radically *insecure*. Not only does the IoT pose risks to people's physical safety in ways that the traditional internet does not, but the fact that its components are *in the world* means it is particularly vulnerable. Add to this the *intensity* of an attack rising from the sheer numbers of IoT devices. Further, as the IoT will require AI to help coordinate components and systems, the decision making may be *inscrutable* which makes for further risk of the second order impacts of cyber-terrorism. Finally, as the IoT is going to be *invisible*, not only will we overlook the components, networks and people involved in its operation, we will also overlook the risks. Combining these five features together, we face an emergent risk from the IoT.

The underpinning factor of how successful IoT enabled cyber-terrorism is, is how resilient the system is to such attacks [27, 28]. By recognising that the IoT is a potential enabler for cyber-terrorism, we are part of the way to reducing the impact of such attacks. The inventory of five features allows us to better understand the risks posed by the IoT. Moreover, by recognising that the IoT is radically insecure, situated in the world, can enable intense outcomes, has elements that are inscrutable, but its risks are invisible, we are better able to understand the ethical responsibility

[13] Michael Zimmerman's original quote is "most would say (and I would again be inclined to agree) that Perry is not to blame for paralyzing Doris, unless he is to blame for his ignorance" [56, 411].

for anticipating and mitigating the risks of cyber-terrorism. So, while I have argued that cyber-terrorism will happen, we do not have to passively allow the terrorists to exploit the vulnerabilities in the IoT. Better design, effective coordinated oversight and a wider public awareness of the risks posed by IoT should help mitigate those risks.

References

1. AAP (2019) Google listens to user speaker recordings. SBS News. https://www.sbs.com.au/news/google-listens-to-user-speaker-recordings
2. Albahar M (2017) Cyber attacks and terrorism: a twenty-first century conundrum. Sci Eng Ethics Online First, 1–14. doi: https://doi.org/10.1007/s11948-016-9864-0
3. Allhoff F, Henschke A (2018) The Internet of things: foundational rthical issues. Internet Things 1–2:55–66. https://doi.org/10.1016/j.iot.2018.08.005
4. Allhoff F, Henschke A, Strawser BJ (eds) (2016) Binary bullets: the ethics of cyberwarfare. Oxford University Press, Oxford
5. Awan I, Imran A (2017) Cyber-extremism: Isis and the power of social media. Society 54(2):138–149. doi: https://doi.org/10.1007/s12115-017-0114-0
6. Bajak F (2020) Suspected Ransomware attack Hobbles Major Hospital Chain's U.S. Facilities. PBS News Hour, 29 September. Accessed 29 April 2021. https://www.pbs.org/newshour/nation/suspected-ransomware-attack-hobbles-major-hospital-chains-u-s-facilities
7. Blanco JM, Cohen J, Nitsch H (2020) Cyber intelligence against radicalisation and violent extremism. In: Babak A, Douglas W, Blanco JM (eds) Investigating radicalization trends: case studies in Europe and Asia. Springer International Publishing, Cham, pp 55–80
8. Bogle A (2018) Strava has published details about secret military bases, and an Australian was the first to know. ABC News, 30 January. http://www.abc.net.au/news/science/2018-01-29/strava-heat-map-shows-military-bases-and-supply-routes/9369490
9. Burmaoglu S, Saritas O, Yalcin H (2019) Defense 4.0: Internet of things in military. In: Emerging technologies for economic development. Springer, Heidelberg, pp 303–320
10. Chapman E, Uren T (2018) The Internet of insecure things. Australian Strategic Policy Institute, Canberra
11. Chu G, Apthorpe N, Feamster N (2019) Security and privacy analyses of Internet of things children's toys. IEEE Internet Things J 6(1):978–985. https://doi.org/10.1109/JIOT.2018.2866423
12. Coady CAJ (Tony) (2004) Defining terrorism. In: Primoratz P (ed) Terrorism: the philosophical issues, pp 3–14. Palgrave, Basingstoke
13. Coady, CAJ (Tony) (2008) Morality and political violence. Cambridge University Press, Cambridge
14. Dang LM, Piran Md, Han D, Min K, Moon H (2019) A survey on Internet of things and cloud computing for healthcare. Electronics 8(7):768
15. de Haan W (2008) Violence as an essentially contested concept. In: Body-Gendrot S, Spierenburg P (eds) Violence in Europe. Springer, Heidelberg
16. Droogan J, Waldek L (2016) Where are all the cyber terrorists? From waiting for cyber attack to understanding audiences. 2016 Cybersecurity and cyberforensics conference (CCC), Aug. 2016, pp 2–4
17. Fernández-Caramés T, Paula F (2020) Teaching and learning IoT cybersecurity and vulnerability assessment with Shodan through practical use cases. Sensors 20(11). doi: https://doi.org/10.3390/s20113048
18. Fletcher D (2015) Internet of things. In: Blowers M (ed) Evolution of cyber technologies and operations to 2035. Springer, Dordrecht, pp 19–32

19. Frazer E, Hutchings K (2019) Can political violence ever be justified? Polity Press, Cambridge
20. Friedman B, David Hendry G (2019) Value sensitive design: shaping technology with moral imagination. MIT Press, Cambridge
21. Ghosh I (2020) AIoT: when artificial intelligence meets the Internet of things. Visual Capitalist, 12 August
22. Gill P, Horgan J, Hunter ST, Cushenbery LD (2013) Malevolent creativity in terrorist organizations. J Creat Behav 47(2):125–151. https://doi.org/10.1002/jocb.28
23. Habibzadeh, H, Dinesh K, Shishvan OR, Boggio-Dandry A, Sharma G, Soyata T (2019) A survey of healthcare Internet-of-things (HIoT): a clinical perspective. IEEE Internet Things J 7(1):53–71
24. Haynes J, Ramirez M, Hayajneh T, Bhuiyan MZA (2017) A framework for preventing the exploitation of IoT smart toys for reconnaissance and exfiltration. International conference on security, privacy and anonymity in computation, communication and storage
25. Henschke A (2017) Ethics in an age of surveillance: virtual identities and personal information. Cambridge University Press, New York
26. Henschke A (2017b) The Internet of things and dual layers of ethical concern. In: Patrick L, Keith A, Ryan J (eds) Robot ethics 2.0: from autonomous cars to artificial intelligence. Oxford University Press, Oxford
27. Henschke A (2020) Trust and resilient autonomous driving systems. Ethics Inform Technol 22:81–92. https://doi.org/10.1007/s10676-019-09517-y
28. Henschke A, Ford SB (2016) Cybersecurity, trustworthiness and resilient systems: guiding values for policy. J Cyber Policy, 1–14. doi: https://doi.org/10.1080/23738871.2016.1243721
29. Ingram HJ (2014) Three traits of the Islamic State's Information Warfare. RUSI J 159(6):4–11. https://doi.org/10.1080/03071847.2014.990810
30. Ingram HJ (2015) The strategic logic of Islamic state information operations. Aust J Int Aff 69(6):729–752. https://doi.org/10.1080/10357718.2015.1059799
31. Ingram HJ (2017) An analysis of inspire and Dabiq: lessons from AQAP and Islamic State's Propaganda War. Stud Confl Terror 40(5):357–375. https://doi.org/10.1080/1057610X.2016.1212551
32. International Data Corporation (2015) Explosive Internet of things spending to reach $1.7 trillion in 2020. According to IDC
33. Jenkins R (2013) Is Stuxnet real? Does it matter? J Mil Ethics 12(1):68–79
34. Ji W, Xu J, Qiao H, Zhou M, Liang B (2019) Visual IoT: enabling Internet of things visualization in smart cities. IEEE Netw 33(2):102–110
35. Kroes P (2009) Technical artifacts, engineering practice, and emergence. In: Krohs U, Kroes P (eds) Functions in biological and artifical worlds: comparative philosophical perspectives. MIT Press, Cambridge
36. Laqueur W (1977) A history of terrorism. Transaction Publishers, New Brunswick
37. Lazarescu M (2016) Hacked by your fridge: the Internet of things could spark a new wave of cyber attacks. The Conversation, 7 October
38. Manjikian M (2017) Cybersecurity ethics: an introduction. Routledge, London
39. Matyszczyk C (2015) Samsung's warning: our smart TVs record your living room chatter. CNet, February 8. Accessed 20 April 2016. http://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/
40. Mayer M, Baeumner AJ (2019) A megatrend challenging analytical chemistry: biosensor and chemosensor concepts ready for the Internet of things. Chem Rev 119(13):7996–8027
41. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A (2019) IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J 6(5):8182–8201. https://doi.org/10.1109/JIOT.2019.2935189
42. Miller V, Hayward KJ (2018) 'I did my bit': terrorism, tarde and the vehicle ramming attack as an imitative event. Br J Criminol 59(1):1–23. https://doi.org/10.1093/bjc/azy017
43. Newman P (2020) The Internet of things 2020: here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue. Business Insider, 7 March. https://www.businessinsider.com/internet-of-things-report?IR=T

44. Peresin A, Cervone A (2015) The Western Muhajirat of ISIS. Stud Confl Terror 38(7):495–509. https://doi.org/10.1080/1057610X.2015.1025611
45. Pramanik PKD, Pal S, Choudhury P (2018) Beyond automation: the cognitive IoT. Artificial intelligence brings sense to the Internet of things. In: Arun Kumar S, Thangavelu A, Meenakshi Sundaram V (eds) Cognitive computing for big data systems over IoT: frameworks, tools and applications, pp 1–37. Springer International Publishing, Cham
46. Primoratz I (2004) What is terrorism? In: Igor Primoratz (ed) Terrorism: the philosophical issues, pp 15–27. Palgrave, Basingstoke
47. Redden M (2016) Tech company accused of collecting details of how customers use sex toys. The Guardian, 14 September. https://www.theguardian.com/us-news/2016/sep/14/wevibe-sex-toy-data-collection-chicago-lawsuit
48. Rid T (2013) Cyber war will not take place. Hurst & Company, London
49. Robbins S (2019) A misdirected principle with a catch: explicability for AI. Minds Mach 29(4):495–514. https://doi.org/10.1007/s11023-019-09509-3
50. Robbins S, Henschke A (2017) Designing for democracy: bulk data and authoritarianism. Surveill Soc 15(3):582–589
51. Schiffer Z (2019) Smart TVs are data-collecting machines, New Study Shows. The Verge, 11 October. https://www.theverge.com/2019/10/11/20908128/smart-tv-surveillence-data-collection-home-roku-amazon-fire-princeton-study.
52. Schmitt MN (ed) (2013) Tallinn manual on the international law applicable to cyber warfare, Cambridge.
53. Song H, Rawat DB, Jeschke S, Brecher C (eds) (2017) Cyber-physical systems: foundations, principles and applications. Elsevier, London
54. Thebault R (2019) Woman's stalker used an app that allowed him to stop, start and track her car. Washington Post, 6 November. https://www.washingtonpost.com/technology/2019/11/06/womans-stalker-used-an-app-that-allowed-him-stop-start-track-her-car/.
55. West E (2019) Amazon: surveillance as a service. Surveill Soc 17(1/2):27–33
56. Zimmerman MJ (1997) Moral responsibility and ignorance. Ethics 107(3):410–426