CONFLICT STUDIES
RESEARCH CENTRE

Cybersecurity, Critical Infrastructure, and Ethics

Adam Henschke

January 2022

Conflict Studies Research Centre
Brook Farm, Lower Benefield, Northamptonshire PE8 5AE UK
www.conflictstudies.org.uk
T: +44 (0) 1865 524 534

EXECUTIVE SUMMARY

This report looks at cybersecurity through a number of layers of analysis. It starts with a discussion of the key ideas and concepts involved in cyberspace and critical infrastructure. The report then sets out the similarities and differences between ethics, values, and rights. It then looks at the idea of international norms to show that there are norms in cyberspace. It next covers particular ethical issues around cyberwar and matters of state–state conflict in cyberspace that fall short of war. State–citizen relations are explored. Ethical issues concerning individuals and cybersecurity are examined and a range of emerging technologies for enhancing critical infrastructure are explored. The report finishes with a set of recommendations for how to apply these theoretical ethics to practical challenges facing cybersecurity and critical infrastructure.

Cybersecurity is presented here as the study of, and interest in, how cyberspace and its underlying software and hardware are the target and/or the means of risks and threats, and what means and ways are available to protect against those risks and threats. Critical infrastructure is defined as shared means that enable us to achieve ends that are essential or have especially important purposes. In a national security context, such infrastructure is critical for the survival of the nation. Ethics is the sustained and rigorous analysis of what we judge to be wrong or right, impermissible, permissible or obligatory.

The driving question is what special features of the cyberenabled environment and related critical infrastructure create novel ethical issues? This allows for a series of layers of analysis: 1) cyberconflict in relation to warfare, 2) the ethics of subwar state–state cyberconflict, 3) the domestic layer, where state–civilian relations play a key role, and 4) the individual layer, to see how ethics and cybersecurity relate to individuals. The report then looks to the cluster of emerging technologies that are playing increasingly pivotal roles in the development of critical infrastructure: artificial intelligence, quantum computing, and cyberenabled physical systems.

To put these concepts into practice, and to offer practical guidance in how to navigate the ethical challenges faced with cybersecurity critical infrastructure, a guide to ethical decision making is presented. The steps are:

1) Clarify the concepts and values that you are working with
2) State the problem
3) Check the facts
4) Identify the relevant factors
5) Develop a list of options
6) Test options by reference to: harms, rights, reversibility, publicity, defensibility, colleagues, professional standards, and organisation
7) Make a choice and act
8) Review steps 1 – 7

The specifics underpinning this guide to ethical decision making for cybersecurity and critical infrastructure are explained through the following report.

Dr Adam Henschke is Assistant Professor at the Department of Philosophy, University of Twente, Netherlands.

Acknowledgements
I would like to acknowledge the Australian Department of Foreign Affairs and Trade (DFAT) for their support for this report. I would also like to acknowledge the Australian Department of Defence (DoD) Strategic Policy Grants, Program Category 1, 2019. I would also like to acknowledge the Australian Research Council (ARC) Discovery Grant DP180103439. All views in this report are my own and do not reflect that of DFAT, DoD, the ARC or any other funding body.

I would also like thank Fritz Allhoff, Shannon Ford, Patrick Lin, CJ O'Connor, Merten Reglitz, and Scott Robbins for insightful comments, suggestions, and feedback on this report. I also note that this report draws in part from (Henschke 2019).

Published by
Conflict Studies Research Centre
Brook Farm
Lower Benefield
Northamptonshire PE8 5AE
UK

ISBN 978-1-908428-14-1

Please cite as: Adam Henschke, *Cybersecurity, Critical Infrastructure, and Ethics*, Conflict Studies Research Centre, Northamptonshire, 2022.

CYBERSECURITY, CRITICAL INFRASTRUCTURE, AND ETHICS

Contents

Cybersecurity, Critical Infrastructure, and Ethics

Key Concepts

Cybersecurity, Cyberspace and Critical Infrastructure

Discussions of cybersecurity are complex as finding a single definition of "cybersecurity" is problematic. Any definition turns on two prior complex and contested concepts; "cyberspace" and "security." Moreover, the particularities of a definition likely depend on the context, the individual, and their particular interests. Cybersecurity for a software engineer is going to differ from cybersecurity for a lawyer, for a military strategist, and so on. The NATO Cooperative Cyber Defence Centre of Excellence glossary has 56 definitions for cybersecurity from 40 different countries and international institutions (Henschke 2019). Within countries, different government departments offer and use different official definitions – the United States, for example, has at least six different official definitions (Henschke 2019). Given this range, a deliberately broad description of cybersecurity is offered here: cybersecurity is the study of, and interest in, how cyberspace and its underlying software and hardware are the target and/or the means of risks and threats and of what means and ways are available to protect against those risks and threats.

The main feature of cyberspace that makes cybersecurity and ethical discussions of it distinct from ethical discussions of "security" is cyberspace's virtual nature. As it is not physical, how should we understand, compare, and respond to malicious actions in cyberspace? When considering the international level, we need to ask if harms or wrongs in cyberspace compare to those arising from a physical attack, and if so, how? When looking at individuals, we need to consider the sorts of harms cybersecurity failures can present and what sorts of ethical risk are influenced by cyberspace more generally. Though cyberspace is virtual, we can recognise that actions and behaviours

in cyberspace have significant psychological impacts – for instance, strong links between cyberbullying and suicide have been established (Hinduja and Patchin 2019). Despite cyberspace's virtual nature, we are psychologically affected by what happens there (Henschke 2017b, 152-198).

"Critical infrastructure" is a similarly contested term. Infrastructure might be thought of in traditional ways, including things like transport, communication and governance systems (Frischmann 2012, 4). A general way of conceptualising infrastructure is to think of it as resources that "are *shared means to many ends*" (Emphasis original Frischmann 2012, 4). *Critical* infrastructure, then, would be shared means to many ends for essential or especially important purposes. In a national security context, such infrastructure is critical for the survival of the nation. Rather than enter into another discussion of definitions, the important element of critical infrastructure for this report is the way that new information technologies allow critical infrastructure to operate and achieve those ends. In short, we need to see both that cyberspace is critical infrastructure itself and that it plays an increasingly important role in enabling other critical infrastructure.

Cyberspace's constructed nature also presents ethical opportunities. This draws from the idea of Value Sensitive Design (VSD) (Friedman and Hendry 2019). VSD "broadly construed, is the notion that our technologies should actively take into account key moral values at their very initiation. Rather than restrict bad use through laws or with patches/add-ons once a technology is in use, VSD considers moral considerations as integral to the technology's very design" (Henschke 2017d). VSD seeks "to account for human values in a principled and systematic manner throughout the technical design process" (Friedman and Hendry 2019, 4). The point here is that cyberspace's constructed nature gives us opportunities to consciously design the virtual environment in ways that are not simply useful but also realise ethical values.[1]

Understanding Ethics, Values, and Moral Rights

This leads us to discussions of ethics, values, and rights. For the purposes of this report, ethics is generally understood as the sustained and rigorous analysis of what we judge to be wrong or right, impermissible, permissible or obligatory. For instance, while we might say that killing someone is wrong or impermissible, ethics is concerned with giving sustained and rigorous reasons as to *why* killing someone is wrong. However,

[1] This point on ethics and Value Sensitive Design is expanded in (Henschke 2017d).

not just any reason will do. Rather than an explanatory reason, ethics is interested in *justificatory* reasons. (Smith 1987, p. 38, 1994, pp. 94-98). Offering a reason for acting is not enough: if it is to be judged as ethical or not, such a judgment needs to be *justified*. For instance, we might ask if a cyberattack is ethically different from a traditional military attack. An ethical explanation would seek to find if there is any important difference between a cyberattack and a traditional military attack.

Underpinning these ethical explanations are key values. Jonathan Haidt's work proposes that there are "(at least) six psychological systems that comprise the universal foundations of the world's many moral matrices" (Haidt 2012, 211). These foundations are the systems of care/harm, liberty/oppression, fairness/cheating, loyalty/betrayal, authority/subversion and sanctity/degradation (Haidt 2012, 211- 214). On this account, our ethical justifications would need to be founded in at least one of these six systems of value.[2]

Combining the two strands of ethics-as-reason-giving and values, ethics as a discipline is ultimately concerned with giving justificatory reasons for actions and judgements by reference to one or more of the six foundational systems described by Haidt. For instance, we might say that a cyberattack that involves the theft of personal information to blackmail people is ethically problematic because it causes harm, interferes with their freedom, is unfair and so on.

There is an easy connection between rights and this account of ethics, where "[r]ights dominate modern understandings of what actions are permissible and which institutions are just" (Wenar 2020). Rights are about what is permitted and how we structure our social institutions. At their most general, "if a person has a particular right, the demand that the enjoyment of the substance of the right be socially guaranteed is justified by good reasons and the guarantees ought, therefore, to be provided… to have a right is to be in a position to make demands of others" (Shue 2020, 13). They are

[2] Care and harm typically track to utilitarianism, which seeks to maximise happiness and minimise suffering. Liberty and oppression relate to basic issues of individual freedom and autonomy. Fairness and cheating are concerned with justice in both process (e.g., abiding by generally accepted rules) and outcomes. These roughly relate to the schools of ethical analysis of utilitarianism, deontology and justice respectively. In Haidt's view, these three fields are commonly explored and endorsed by those that would be considered in liberal democratic approaches to ethics, skewing towards the left of politics.

Of the remaining three foundations, loyalty/betrayal and authority/subversion are concerned with the commitment to, and deference that one shows to, one's family, community and leaders. The final foundation is sanctity and degradation, which are commonly associated with showing respect to religious icons and traditions; but they can also relate to more secular symbols like showing respect for a country's flag and so on. According to Haidt, these remaining three foundations are more commonly found in politically and socially conservative groups and cultures, where patriotism, nationalism and the importance of community over the individual are seen as valuable.

typically associated with individuals, and how those individuals order their relations with others and how the given society supports and constrains individuals in their actions.

Rights may have their foundation in these six sets of moral values - what we might call moral rights or human rights - but rights can also refer to political, social or legal rights. At a very general level, the idea of moral rights typically contains two common elements: entitlement, and value. First, as persons, we are all entitled to certain rights. Moral rights are often thought to be general or universal. Every person has such rights, regardless of where they are. Thus moral rights are thought to be *universal*. For instance, many hold that people everywhere have a right to not be tortured (Davis 2005, Sussman 2005). It does not matter if I am in Australia, an Australian in another country, or a foreign citizen in Australia, I simply should not be tortured.

The second element of a moral right is that it denotes something of deep significance or moral value. To claim that I have a right against something or to something is to express a belief that that something is of extreme significance. The right against torture is not something comparable to a claim that I should get a cheap price on a book. One of these is of extreme significance whereas the other is only of limited importance. "Justifications for human rights should defend their main features including their character as rights, their universality, and their high priority" (Nickel 2019). An ethical analysis would therefore offer a reason or set of reasons justifying why a right against torture is in fact a right – it causes extreme suffering, it violates my personal freedom, it is unjust and so on. In contrast, the justifications for getting a cheap book would likely be a lot thinner. One could say that I have a right to education, for instance, because being educated improves my welfare, enhances my freedom, is necessary for a fair distribution of resources and so on. But one would then have to make a special argument why *this* book is necessary for the realisation of those values.

For instance, Merten Reglitz argues that free internet access should be considered a universal moral right. He offers reasons for this claim by suggesting three interrelated justifications:

(a) "[Free internet access] is necessary for individuals to meaningfully influence global players who make global rules;
(b) In an increasingly global and virtual world, [free internet access] is already uniquely effective for the realisation of important political human rights (free speech, free association, and information); and

(c) If it would be governed appropriately, it would be extremely effective in protecting other basic human rights (i.e., life, liberty, and freedom from torture)" (Reglitz 2019, 314-315).

Understanding Political, Social, And Legal Rights

In contrast to the idea of moral rights being universal, *political* and *social* rights are formed and expressed, in part, via the political and social context in which people live. These often (but not always) also have a moral basis but can be defined and enshrined differently in different countries. They might be considered as political rights such as those "that protect people's liberty to participate in politics by assembling, protesting, voting, and serving in public office… [or] [e]quality rights that guarantee equal citizenship, equality before the law, and freedom from discrimination… [or] [s]ocial rights that require that governments ensure to all the availability of work, education, health services, and an adequate standard of living" (Nickel 2019). We can see here that these political and social rights are more comprehensive and complex than simple moral rights claims, dependent on the political institutions of a given nation, the justice of legal institutions and the social welfare and policies of the nation. And in contrast to the moral rights, while the foundations for these political and social rights might be tracked back to one of the foundations listed above, they can only be properly clarified and understood in relation to the political and social context in which the rights claim is being made.

One further possible contrast with moral rights is that political and social rights, while important, can more easily be overridden. "Most civil and political rights are not absolute—they can in some cases be overridden by other considerations. For example, the right to freedom of movement can be restricted by public and private property rights, by restraining orders related to domestic violence, and by legal punishments. Further, after a disaster such as a hurricane or earthquake free movement is often appropriately suspended to keep out the curious, permit access of emergency vehicles and equipment, and prevent looting" (Nickel 2019).

Finally, we have *legal* rights. These are the formalised instantiations of moral, political, social and other claims. Importantly, where legal rights differ from moral rights is that they are unlikely to be considered general or universal. As an Australian citizen I have a set of legal rights that would not necessarily be recognised in a jurisdiction

outside of Australia. For instance, while I might have a legitimate claim to fair political processes and representation and have legal rights in Australia that endorse and protect those claims, I cannot vote in another country's elections. My legal right only extends as far as the law allows. Legal rights are typically much more specified than moral, political or social rights. And much more constrained. Again, however, they share the notion that – even if they might be outweighed by other considerations – they are still of significance and importance. In this way, calling something a right is generally a shorthand to signify something of special importance, where the burden of the argument falls on the person who might diminish or violate the rights of the person making the claim.

As a final point here, we need also to recognise that ethics and the law are concerned with two different aspects of human relations. What is legal might not necessarily have ethical content, and what is ethical might not necessarily be covered by the law. For instance, consider the law that we drive on left hand side of the road in Australia. There is no ethical reason why we should drive on the left or the right-hand side of the road, though there are ethical reasons to follow the law. Or consider that I play a regular card game with friends, but it turns out I have been cheating them. While my cheating is likely unethical, it is not something that one would call the police over, though in some situations like professional sports matches, there may be laws to prohibit cheating. The point is that ethics and the law differ.

This discussion is relevant to issues of cybersecurity, cyberspace and critical infrastructure in a range of ways. If one is to advocate or seek to advance a moral or human rights-based understanding of cyberspace, one would be bound to the ideas that these rights are universal – they are owed to every person, regardless of their location or citizenship. A political or social rights approach view might see rights claims as being in part related to the political or social context in which the claim is being made, and a legal rights approach would likely limit those rights to a particular jurisdiction. On all approaches, however, calling something a right denotes that it has special importance, and there would need to be some significant reasons given for why that rights claim should be overridden.

We might now ask if there are ethics in cyberspace. As will be detailed through this report, there are many areas where issues of ethical importance exist in cyberspace, requiring the need for justifications of one's actions by reference to foundational values. In relation to rights, in recent years as people's lives have increasingly become

integrated with cyberspace, there have been a number of efforts domestically and internationally to apply rights concepts to cyberspace. The European Union, for instance has sought to legitimise claims to a right to be forgotten, and with the General Data Protection Regulation (GDPR), put in provisions to respect rights to privacy and anonymity. Scholars like Reglitz claim that access to the internet is itself a basic human right (Reglitz 2019, 314-315). Depending on how one understands rights, they may be universal and held by all individuals or they may be legal and constrained to one's own national jurisdiction. However, the interesting aspect is how the growth and evolution of cyberspace has prompted such rights claims about cyberspace and people's access to it.

International Norms and Cybersecurity

The virtual nature of cyberspace makes it distinct from physical space. It is distinct from geography and national boundaries; cyberspace exists or overlays international spaces. Given this combination of its virtual nature and being outside of geography, we need to ask first if there are any norms of behaviour in cyberspace. Without such norms, a discussion of ethics and cybersecurity would be limited. The core function of norms "is to make us *accountable* to one another… What accountability involves is others having a recognised right or entitlement to determine how one is to behave… It is not that we have information about what others will do. Rather, we are in a position to hold one another to account and to demand and expect things of one another" (Brennan et al. 2013, 36). This is obviously in keeping with the account of ethics as reason giving and fits with a 'thin' idea of rights, where a rights holder is at very least owed an explanation, and perhaps a justificatory reason, as to why someone else's actions are justified.

Though there is disagreement about what norms apply to cyberspace at an international level, there is an emergence of norms for cyberspace. The mechanisms of emergence may be, as Michael Schmitt and Liis Vihul argue, top down (Schmitt and Vihul 2016), or as George Lucas, Jnr. argues, bottom up (Lucas Jnr 2016a), or a combination of both. Starting at this international level, while recognising that international norms are contested, as of 2018, the Budapest Convention on Cybercrime has been ratified by 57 states, with four more signing but not ratifying this agreement dedicated to international cooperation on internet and computer crime. This suggests that there is, at the very least, a norm of cooperation in cyberspace. Australia for instance has signalled that it holds not only that there are norms in cyberspace, but has publicly advocated for, and seeks to support, 11 norms identified by the UN Group of

Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security (Commonwealth Of Australia 2017).

Another suggestion is that aspects of international law may apply to cyberspace. Drawing from a notion of equivalence, a group of international legal scholars published the Tallinn Manual on the International Law Applicable to Cyber Warfare to present a detailed analysis of when and how existing international law applies to conduct in cyberspace (Schmitt 2013). The Tallinn Manual sought to apply the "norm of equivalence": if a cyberattack causes physical damage equivalent to a kinetic or "traditional" military attack, then it should be considered the same. Thus, if a cyberattack causes physical damage that meets and surpasses the level of an armed attack, this could be considered an act of aggression. The authors of the Tallinn Manual themselves note that it is not legally definitive (Schmitt 2013); however it gives a solid foundation for the notion that international law applies to cyberspace. Again, the point here is that there is a slowly emerging consensus that, far from being free of norms, cyberspace is an area where there are norms of behaviour, even at an international level.

In contrast, there is a view that, despite these many efforts to impose norms on cyberspace, there are presently no actual norms in cyberspace, just proposed ones. Hackers and other bad actors in cyberspace don't seem to be constrained by much, even basic decency, as they continue to target and prey on some of the most vulnerable people; for instance, ransomware attacks on hospitals during a global pandemic are still occurring (Muthuppalaniappan and Stevenson 2020). At the same time, law enforcement is severely limited in cyberspace, and the majority of cyberattacks, especially high-profile ones, continue to go unprosecuted and unpunished. Thus, cyberspace could be seen as a chaotic *frontier* of sorts, and laws and norms are always unclear or contested on frontiers (Lin 2016). In any case, to everyone but perhaps the most die-hard anarchist, there's a real desire and need to tame this frontier – to establish norms and law and order in cyberspace, given that the stakes can be very high.

Ethical Challenges in Cyberspace and for Critical Infrastructure

Cyberwarfare

Following from the recognition that some norms apply or should apply in cyberspace, and in the way we ought to think of critical infrastructure, the "just war" approach supplies content to the norms through adaptation of its criteria to cyberspace. The just war tradition in philosophy is a major influence, if not basis, for the laws of armed conflict and international humanitarian law.[3] In his influential 2013 book, *Cyber War Will Not Take Place*, Thomas Rid argues that because cyberattacks are, strictly speaking, confined to cyberspace, they are not violent and therefore not strictly warfare (Rid 2013, 1-34). The virtual nature of cyberspace, Rid argues, should give us significant pause when calling cyberattacks "warfare." Rid's position has been widely discussed and criticised; see for instance (Allhoff, Henschke, and Strawser 2016). Adding complexity to these arguments, cyberweapons have been shown to impact the physical realm. Stuxnet was a complicated computer virus that caused physical destruction in the centrifuges that were part of the Iranian nuclear program (Langner 2013).

Stuxnet is important because it shows that cyberattacks can lead to physical outcomes: cyberattacks have the capacity to physically impact critical infrastructure. Also, it is widely suggested that the complexity and skills needed to develop Stuxnet were the province of state actors (Langner 2013). Stuxnet's relevance is that it provided proof that cyberattacks are not confined to cyberspace. Even bearing in mind Stuxnet, it is important to note that no single, stand-alone cyberattack has been deemed to be an armed conflict – no pure cyberattacks have equated to or led to traditional state-on-state warfare. In contrast, cybermeans have been used to augment and enhance traditional military activities; for example, a series of hybrid military attacks occurred in Georgia and Ukraine that utilised cybercapabilities and traditional military forces (Schmitt 2011).

Would a cyberattack that has its primary effects within cyberspace justify a kinetic response? That is, does a pure cyberattack constitute a just cause for war? A necessary condition for a just war is a just cause, typically self-defence against armed attack (May 2008). The special challenge of cyberattacks is the issue of commensurability of impacts – how do you weigh virtual harms versus real world

[3] For more on just war, see (Coady 2008, Coates 1997, Coleman 2013, Glover 2000, May 2007, 2012, McMahan 2009, Orend 2013, Steinhoff 2007, Walzer 2006, Allhoff, Henschke, and Strawser 2016, Allhoff, Evan, and Henschke 2013)

harms? In 2007 the Estonian capital Tallinn was subjected to a comprehensive and sustained cyberattack whose direct effects were restricted to cyberspace (although other hostile actions by Russia had direct effects in the physical world) but which had significant mediated impacts on the government and provision of government and commercial services like banking and was significantly disruptive to civil society (Schmitt 2011). Following these cyberattacks, some called for physical attacks against Russia. These calls raised the vexing issue of commensurability of harms: is it ethically justifiable to respond with physical force to an attack whose primary impacts are virtual? To date, no such response has occurred, suggesting that people generally hold virtual impacts to be incommensurable with physical ones.

Attribution is another unique aspect of cyberattacks. For a long time, cyberspace's virtual nature meant that an attacker could disguise their identity online, and so cyberattacks were quite hard to attribute to a specific person or source (Rid 2013, Schmitt 2011). Moreover, the nongeographic nature means that cyberattacks can originate from anywhere. This has ethical implications because if a country subject to cyberattack was to hit back with either cyber or kinetic means, and they misattribute the source of the initial attack, they may themselves then to be in contravention of the ethics of war, which could lead to international condemnation, United Nations (UN) sanction, or even attack, as per Article 51 of the UN Charter.[4]

A further set of issues centre on the state's responsibility to provide cyberdefence to its citizens (Henschke 2017a). Historically, in a context of traditional military conflict, a state's responsibility was not simply to use military means to respond to an aggressor's attack, but also to provide some level of civil defence against the aggressor. In the lead-up to and during World War II, for instance, the UK had a series of civil defence measures and practices: provision of 30–40 million gas masks for at-risk population centers, pumps to prevent the spread of fires from German bombing and the development and supply of the "Anderson": an air raid shelter for households (Henschke 2017a). The point here is to recognise that first, a state may have a duty to prepare and defend its citizens against cyberattack. Second – as will be discussed below – that such efforts run into issues of privacy and state overreach. Note that if we take the view that there is a human right to internet access, this entails duties for states to protect cyberspace from outside attacks, because otherwise citizens can't use the online sphere safely and have their rights respected while being online.

[4] For more on this, see: (Ruys 2010).

Beyond its physical impact, Stuxnet is of ethical interest as it was highly discriminatory – although it was spread widely around the world, its design meant that only one specific target, the centrifuges of the Iranian nuclear program, would be affected.[5] Discrimination is a key criterion of the just war tradition's *jus in bello* set of criteria (McMahan 2009, Orend 2013), and Stuxnet is potentially a weapon that has this key ethical principle designed into it. This presents one way to think of VSD; cyberweapons can be designed such that the just war principle of discrimination is designed into the weapon in ways that traditional weapons cannot.

Another way of looking at ethically grounded principles like the *jus in bello* criteria is to see that cyberweapons do not so much give us the capacity to design these values in, but that they reveal our existing values and core ethical beliefs. For instance, "if offered the choice to use a cyberweapon or not as part of a traditional military operation, should a commander favour the targeting of civilians or causing physical damage? This problem highlights a tension in just war theory's *jus in bello* criteria: that on the one hand, a decision maker should adhere to the principle of discrimination, while on the other, they should respect the principle of proportionality" (Henschke 2017e, 227). The "core tension is that discrimination and proportionality are both important moral values" (Henschke 2017e, 239).

This is not a special problem for cyberweapons or cyberwarfare, but a more general issue faced in military ethics and by military decision makers as a matter of course. "Technologies present us with the problem of deciding from within a new set of options, thus making us rethink how we normally make these decisions. This then makes us think about the values underpinning those normal decision-making processes. That is, the options new technologies offer that can *challenge* what we take for granted… rather than just posing a challenge to one's existing moral beliefs, the new options offered by technology *reveal* those existing beliefs about which values take precedence over other values, and which moral theory is best suited to resolve our issues" (Henschke 2017e, 240-241). That is, while our ethical principles can and should guide us in how we design and deploy cyberweapons, these new technologies also force us to reflect on how we normally make ethically relevant decisions, and can reveal which of the ethical values we take to be more or less important. When our values are revealed, we are forced to ask whether we should hold or change those values. The point here is that new technologies can be a tool for ethical reflection, in ways that can make us rethink our existing ethical beliefs. This is core to the notion of ethics as seeking

[5] I recognise here that Stuxnet did spread to other infrastructure, though it did not cause damage to them.

not simply to justify our ethical judgements, but to properly revisit and rethink those judgements.

Peacetime Cyberconflict Between States

In 2017, a follow-up to the Tallinn Manual, the Tallinn Manual 2.0, was released (Schmitt and Vihul 2017). It built on the recognition that though cyberwarfare is possible, the majority of state–state conflicts in cyberspace occur at a level below that of an armed attack. Tallinn Manual 2.0 thus "examines key aspects of the public international law governing 'cyber operations' during peacetime" (Schmitt and Vihul 2017, 3). If a cyberattack does not rise to the level of an armed attack, and so kinetic warfare is not the ethically appropriate response, what should be done about foreign state cyberattacks?

Spying, espionage, and related state peacetime conflict are hardly novel. What cyberspace does is increase the vulnerability of targets to attack, and the capacity for actors to attack remotely – what Rid (Rid 2013, 81-138) describes as espionage and subversion. Given that so much modern behaviour and social interactions occur either in or through cyberspace, the scope of state surveillance and espionage is orders of magnitude greater than in the past (Henschke 2017b, 217-251). Many innocent civilians' personal information has been accessed and analysed by state security agencies in great quantities (Greenwald 2014, 90-169). While certain state surveillance programs were perhaps ethically permissible in the past, we now face surveillance programs that involve data gathering in many orders of magnitude greater than was previously possible. This difference in magnitude offered by cyberspace shifts our ethical calculations about the permissibility of state espionage and surveillance. Though surveillance and espionage that are targeted at individuals suspected of significant crimes and/or of being foreign agents might be justifiable, given sufficient oversight and constraint, widespread untargeted surveillance is not (Greenwald 2014, 251, Henschke 2017b, 245-251).

Following the election of Donald Trump in 2016 as President of the United States, there has been concern about and scrutiny of actors suspected to be working for Russia as part of a large-scale "foreign influence operation" (Mueller 2018). In and of itself, this is hardly new; for instance, subversion through foreign influence operations was arguably a common practice during the Cold War (Rid 2020, 61-312). The 2016 United States presidential election, however, demonstrates the increased vulnerability of states to subversion campaigns conducted through cyberspace. Cyberspace's nongeographic

nature – the way it allows actors to hide their identity, and the many critical social and political processes that are integrated with cyberspace – make state-based political subversion campaigns much easier, cheaper and more effective than in the past (Rid 2020).

Two key ethical issues arise here. First, should states engage in such operations at all? On the one hand, such operations go against the very notion of the sovereignty of other states. Efforts to influence and subvert a foreign country's political processes are significant violations of the target state's right to self-determination. On the other hand, if the target state's government is violating the core rights of its people, then it may be that they have lost the moral authority to govern, and thus intervention is warranted (Altman and Wellman 2009). However, in line with the idea of ethics as justification, any such efforts at foreign subversion would need to be founded in sound reasoning. Moreover, given the traditions of respecting national sovereignty and the importance of the integrity of political processes, any such justification would need to be quite significant and come with a range of significant constraints.

Rather than a state going to war and killing people, cyberspace offers an option for it to achieve a just cause without recourse to physical violence, and so subversion through cybermeans or that target critical infrastructure in non-destructive ways may adhere to the just war criterion of last resort. The ethical issue here concerns what Lucas calls "state-sponsored hacktivism" (Lucas Jnr 2016b): the worry is that by lowering the bar for state–state subversion, active cybermeasures are used more frequently and without sufficient justification. In order to be ethically justified, regime change requires more than simply a disagreement with the given regime; just like the case of responsibility to protect, something like significant systemic rights violations would be required for interventions (Altman and Wellman 2009, Thakur 2016), even if those interventions are through cyberspace.

A further question is how should states respond to such subversive interventions? If it is revealed that a foreign power has been seeking to subvert core political processes like elections, what is a state ethically justified to do in response? Even if we agree that physical force is not justified, can a state respond in kind, by actively seeking to subvert the other state's political processes? The recognition of a norm like proportionality means the risks of increased conflict through escalation of responses and counter-responses needs to be factored into any decision to use cybercountermeasures. Cyberspace increases states' vulnerability to subversion, and makes such operations easier (Rid 2020, Henschke, Sussex, and O'Connor 2020). Though the norms of behaviour are still emerging at the international level, the

increased power and scope of surveillance and risks of escalation are core ethical concerns for any decision-making here.

Another ethical challenge highlighted by cybersecurity arises in the ways that states treat citizens and noncitizens differently. When the Edward Snowden revelations first came out, the then-chair of the US Senate Select Committee on Intelligence, Senator Diane Feinstein, stated that the programs were alright because they did not put United States citizens under surveillance. Many legal regimes around the world restrict state surveillance of citizens while permitting surveillance of noncitizens. The ethical foundation of this distinction is complex: on the one hand, if we see certain moral rights as universal, then recognition of the right to privacy should not depend on citizenship (Nickel 2019, Wenar 2020), a point reinforced by the UN recognising a human right to privacy. On the other hand, if a state is constrained in what it can do to its own citizens in virtue of something like a social contract, then partialism and deference to one's own citizens may be justified. Cyberspace's nongeographic nature puts significant pressure on the citizen/noncitizen distinction[6] and forces us to reconsider why such a distinction exists.

In the moral or human rights approach, the fact that one person is a citizen and another person is not should not matter at all. Insofar as privacy is a fundamental moral right, then one's citizenship is irrelevant – you are afforded the protection granted by the right to privacy regardless of where or who you are. In the legal rights approach, however, the claim to privacy is bounded by the jurisdiction one is affiliated with. Thus, the particular rhetoric a government uses matters – if a government advocates the view that moral or human rights exist, and that they must be respected in cyberspace as well as in the physical world, then they are bound by consistency to hold that all people everywhere have those rights. This would mean that, in the human rights approach, the government should not violate other people's right to privacy and should criticise those governments that do.

Coming back to the view of cyberspace as a lawless frontier, where laws and norms are so difficult to enforce that law enforcement, for all practical purposes, does not exist in cyberspace – international law does have something to say here. It recognises the category of "frontier incidents," where minor skirmishes, even if they result in deaths and injuries, are not treated so seriously that a state may invoke its right to self-defence in launching a counteroffensive (Lin 2016). That is, misunderstandings and clashes happen on frontiers, and to recognise and give space for those incidents

[6] Noting here that countries like the US use a broader US Person/Non US-person distinction – a US person includes citizens and anyone residing in the US.

can better promote peace by not allowing them to escalate into outright war. This is consistent to the understanding in the just war tradition that attacks, no matter how serious or provocative, don't *need* to lead to declarations of war or counter-strikes, even if they justifiably could; we could choose not to respond with force.

Cybersecurity in the Domestic Context

Following from the point above, perhaps states cannot spy on their own citizens without sufficient warrant because it is a gross invasion of the right to privacy. This statement draws from the notion of privacy as being distinct from a public space. Here, privacy is seen in a mostly political context, and refers to limits on state intrusion in the space of its citizens (Henschke 2020b, Solove 2008, Nissenbaum 2009, Koops et al. 2016, Henschke 2017b). These arguments turn in part on the capacity of a state to wield power and in some cases violence against its citizens through its police forces and intelligence agencies. The mere threat of such state power and violence, it is argued, can chill personal and social development, impacting on political association and protest (Solove 2008, 178, 193, Greenwald 2014, 173-177, Robbins and Henschke 2017). However, in liberal democracies, police investigations and surveillance typically require some suspicion of illegal activity, and processes like the granting of warrants mitigate the power of the state with its responsibility to provide security to its citizens.

The ethical issues here are traditional issues in political philosophy – what are the responsibilities that a state has to its own citizens, and how far can the state go in service of those responsibilities? For instance, it is common to claim that people have a right to security and that it is the state's primary responsibility to provide that security. On the other hand, liberal democratic states define themselves by reference to the fact that individuals are not only granted particular rights, but have rights as constraints on state activity. Privacy, for instance, does not just refer to an individual's rights against others intruding on their space or accessing their personal information, but also refers to a citizen's rights of non-interference by their government (Henschke 2020b, Zuboff 2019). What cyberspace offers is an unprecedented expansion in state's capacities to violate a citizen's privacy. The question here is not so much should a state do this – again, the idea that a state must afford its citizens a right of security suggests that in certain circumstances such state actions may be justifiable – but *when* and *how* a state should choose security over privacy.[7]

[7] As Solove has argued, in a number of circumstances, this may be a false dilemma, as with good design of our technologies and laws, we might be able to pursue both (Solove 2013).

What ethics as justification by reference to reasons seeks to do is give a coherent and hopefully consistent set of reasons about the trade-offs and balances between claims of security and privacy. "Overarching every form of political community, [justice] not only demands reasons for why someone has or does not have certain rights or goods, but first and foremost it asks how it is determined who has a claim on what and how the participants, understood democratically in their dual role as authors and addressees of justifications, stand in relation to one another" (Forst 2012, 1-2). As a fact of liberal democracy, we need laws and policies that not only ensure that the state's powers are constrained, but assure us that they are constrained (Robbins and Henschke 2017). Again, this is hardly a new ethical or political issue. What cyberspace, and the policies and actions that are currently forming around cyberspace, is doing is forcing us to revisit the foundation of our political communities, to see what the reasons given for favouring security over privacy are, and to see if they are good, coherent and consistent reasons.

Next, as the Snowden revelations show, new information technologies create a cybersecurity risk from insiders. The ethical issues around government leakers and whistleblowers are familiar (Ceva and Bocchiola 2019, Delmas 2015); however, their access to sensitive state and personal information and the capacity to publicly use cyberspace to access, exfiltrate, and distribute large amounts of sensitive information is enhanced and compounded by novel information technologies (Henschke 2017b, 3-27) and the access that these information technologies give to critical infrastructure. This then raises the ethical challenges of what lengths a state can go to in order to identify insider threats and what sorts of punishment, if any, are legitimate for those engaging in leaking and whistleblowing. An extension of this is that any state department, agency or institution must ensure that it actually has effective policies to support whistleblowers and does not punish those who do blow the whistle, nor should it intimidate those who may be considering whistleblowing. Institutions in the "the security sector, in particular, should not simply protect whistleblowers but do more to encourage them" (Henschke 2020d).

Extending from this point is the practical and ethical issue of hiring people in the cybersecurity industry. As Snowden demonstrates, given the technological capacity to gather, remove and distribute controlled information, a disgruntled insider can pose significant risks to an institution, whether government or otherwise. As such, these industries need to be quite careful with their hiring practices. This is arguably even more of an issue for government entities/actors like security, military and intelligence agencies. They typically have a range of vetting processes that an individual must go

through before they can be hired or granted access to secret/top secret information. The problem here is twofold. First, such vetting processes are slow and expensive. And given the time that such hiring can take, it is a frequent issue faced by cybersecurity-related government institutions that they either cannot attract or cannot retain top quality candidates. Not only do government wages compare unfavourably to private industry wages, if someone has to wait months to years before starting the job that they are being hired for, the chances of being headhunted by private industry increase. Second, these vetting practices can, by design, exclude people who have particular criminal or 'anti-social' pasts like hacking. However, many of the best people working in cybersecurity have backgrounds as hackers and the like. If these people are excluded from relevant jobs in government, then the respective agencies are likely to be losing out on some of the best talent.

This is an ethical issue for two related reasons. First, it means that those working for government are perhaps not always the best and brightest in the cybersecurity field. And this suggests that the security provided to citizens by their governments is less than it could be. And if this is the case, the government is perhaps not meeting its obligations to its citizens. A second issue comes out as fairness – if those who have a history of hacking and related activities in cyberspace are excluded from working for the government, they may be suffering an injustice. While criminal and other anti-social behaviour should not be overlooked, if the individuals have served their time or suffered the relevant punishment, then perhaps they should be afforded a second chance?

The problem of fairness in hiring is a larger issue for security agencies. Again, because of the justified need to increase vetting as individuals get hired into more sensitive positions, the documentation needed as part of that vetting increases. What this means is those people from non-local background and/or who have more problematic histories will have lower chances of being hired. What this can produce is a relative monoculture within particular organisations and institutions. This is not only a form of process-driven discrimination, but can also substantially impact the capacity of a given agency to fulfil its mandate. If an intelligence agency is supposed to understand, anticipate and protect against hackers, but it has no people from those communities or cultures and ultimately lacks a deep understanding of these cultures, it will have diminished capacity to discharge those duties. This is an issue that counter-terrorism agencies around the world have faced, so it is not a unique problem for cybersecurity. But with the need for good candidates in cybersecurity related jobs only growing, this is an issue that those working in cybersecurity need to respond to.

Another issue comes from the technologies that allow for easy encryption of data and personal information. Insofar as privacy is a right, encryption technologies may be ethically desirable as they offer citizens protection against surveillance conducted by the state and corporations. Depending on the form of encryption, these technologies may protect the anonymity of individuals, or the content of their communications. The Onion Router (TOR), for example, makes it hard for an outside person to identify the source and target of a communication. Free services like Signal or WhatsApp encrypt the content of a communication. Giving access to un-encrypted metadata may allow an outside agent to know that two people are in conversation, but they will not know what they are talking about.

Such encryption technologies, however, can also protect unethical behaviours and activities. By definition, unethical behaviours and activities should not be conducted. An interesting ethical challenge occurs in the context of state–citizen relations. Can states compel corporations to create "backdoors" in key technologies such that intelligence agencies could bypass the tools of anonymity and encryption? Though national security emergencies may suggest that backdoors are important, the presence of government-accessible backdoors in key technologies would themselves constitute a major cybersecurity vulnerability. Furthermore, following the Snowden revelations, many, like Glenn Greenwald, hold that liberal states (Greenwald 2014, 208-209), as well as authoritarian ones, are not trustworthy; therefore they should not be granted the tools to crack or overcome encryption. A related issue is that anonymity and encryptable services are especially important for dissidents in authoritarian states, so those in liberal democratic states who want to support human rights movements in authoritarian states may need to invest in and support infrastructure like TOR, even though that might present challenges from a domestic security perspective.

At the level of international norms, there is a worry about hypocrisy. Australia, the US and other liberal democratic nations have been highly critical of other nation's constraints on internal information and active and ongoing efforts to hack the ICT infrastructure of other nations and institutions. For instance, one of the chief concerns around 5G mobile phone technology is that it will be a foundational technology for years to come and may pose a significant security hazard, giving the state actors backdoors into all communications (Kaska, Beckvard, and Minarik 2019). However, if countries like Australia require private industry to build in backdoors to encryption, what makes them different from those countries they are criticising?

One obvious point is that Australia is not a totalitarian or authoritarian state; rule of law and legal protections for individual rights are present in Australia. However, this

begs the question: isn't having the capacity to place every individual under surveillance and to monitor private communications arguably the hallmark of an authoritarian state? This brings us back to the issues of human rights – if liberal democracies make public claims to take rights like privacy and free communication seriously, then they need to be very careful with how they approach issues like backdoors and encryption.

Outside of the explicit ethical concern, there is also the loss of moral authority. A liberal democracy loses the moral authority to criticise authoritarian states if it engages in comparable practices. This is not to say that all encrypted communications need to be protected. Rather, the point is that in liberal democracies we need to take special care to ensure that such policies do not undermine our core values and to assure our citizens that these policies are well thought out and necessary (Robbins and Henschke 2017).

A further issue here concerns the relation between intelligence agencies and civil society. Following the Snowden leaks, and in light of the stormy relationship between US President Trump and the US national security agencies,[8] the public interest in intelligence as a practice has surely been heightened by the technical, social and political aspects of cybersecurity; here, it is not so much "what should the public *know* about state espionage operations?", and more about "what should the public *do* about state espionage operations?" Publicity and public engagement here are argued to both *ensure* and *assure* that there are workable constraints on state behavior (Robbins and Henschke 2017).

Cybersecurity and the Ethical Challenges for Individuals

The final set of concerns come at the layer of the personal and individual. Continuing with privacy, rather than seeing privacy as a limit on state intrusion, it can also be conceptualised in how an individual relates to a community or society at large (Koops et al. 2016, Solove 2008). For some, there is no such thing as privacy anymore: Pointing to people's willingness to actively share the most intimate and mundane details of their lives online, in the late 2000s the heads of Google and Facebook suggested that privacy was no longer a social norm (Henschke 2017b, 35). However, ongoing and sustained public criticism of Facebook's use and misuse of people's personal information shows that people do care about who has access to their personal information and what is

[8] For example, former Director of the US National Security Agency and Director of the Central Intelligence Agency, Michael Hayden, former director of the Federal Bureau of Investigations James Comey, and former Director of National Intelligence Agency James Clapper have all released books that include significant criticism of the negative impact of US President Trump on the intelligence community and US national security (Hayden 2019, Comey 2018, Clapper and Brown 2019).

done with it. Secrecy is only one way of thinking about privacy. We can think of it as information control (Koops et al. 2016, Macnish 2018). We can also think of it as caring about intimate information, the protection of data, a necessity for personal development, and, perhaps, as a bundle of these concepts (Henschke 2017b, Solove 2008, Inness 1992). What cyberspace does here is put pressure on some privacy concepts, like secrecy, and force us to revisit and revalue other privacy concepts, like intimacy, personal development, and so on.

In terms of the actions of individuals, the ethics of hacking present another point for analysis. One way of understanding hacking is to look at the motivation of the hackers, variously called "White Hats," "Black Hats," and "Grey Hats" (Manjikian 2017). White Hat hackers are motivated to help their targets. Their actions are intended to identify cybersecurity vulnerabilities and let the targets know of the given vulnerability, such that it can be patched or fixed. Other hackers are motivated for malicious reasons and are called Black Hat hackers. Their actions are intended to harm the targets – for the hacker's own economic gain, for political reasons, to embarrass the target, and so on. A third sort of hackers, called Grey Hat hackers, are also described. Their motivations are harder to categorise, as they may want to identify cybersecurity vulnerabilities in order to receive some reward from the target. In contrast to the White Hats, they do not do this at the request of the target; but, in contrast to the Black Hats, neither do they pose an immediate threat to the target.

This leads us to the fraught ethical issue of "hacking back" (Lin 2016). If a private company or individual has been the target of or victim of a hacking attack, are they ethically permitted to hack back? That is, can they act essentially as a vigilante to find those who targeted them and hack them back? On the one hand, in the absence of their own state responding, perhaps they have a right to take the law into their own hands. This may also act as a warning sign to other hackers, to stop them from hacking people. On the other hand, such hacking back is typically illegal, or at least presumed illegal where existing laws do not specifically address or contemplate hacking back. Moreover, there is the risk that the vigilante hackers target the wrong person. Or that, by hitting back at state sponsored hackers, the private individual might inflame existing geopolitical tensions, leading to an escalation of conflict between states. One of the key problems with private vigilante hackers is that they may lack understanding of whom they are targeting and what responses their actions may cause. That said, private individuals and companies do have a great deal of technical knowledge and can often be far more informed and skilled in the technical aspects of cybersecurity than government agencies (Bowden 2011). The ethical issues here arise in three related

ways. First, does an individual or private company have a right to hack back? Second, does their relevant government have the right to stop or punish private actors when they hack back? And third, do state intelligence agencies have a responsibility to target, stop and punish malicious hackers in order to defend their own citizens?

As witnessed in this report already, how a problem is framed matters (Lin 2016). If we are looking at an issue from, say, the perspective of armed conflict between states, then the resulting judgments may differ if we were to treat the issue as one of terrorism, or frontier incidents, or domestic security, or privacy and so on. For instance, if a cyberattack is framed as part of state-on-state warfare, then private individuals who hack back may transform into "noncombatants directly participating in hostilities" and thus forfeit their rights as noncombatants. If it's framed as a frontier incident, which is governed by more permissive norms (to the extent any norms exist on a frontier), then hacking back would seem to be permitted. The frontier frame is supported by the fact that, given the years of intense cyberattacks suffered by many nations, none of them have escalated tensions to the level of actual warfare, as was feared; this suggests we're more forgiving of transgressions on frontiers where laws and norms are unclear.

Another illuminating frame is cybersecurity as public health. This doesn't depend on viewing internet access as a human right, even if that helps, but it should be clear that connectivity is at least a public good that could be threatened by a mere handful of bad actors. So, there's a natural analogy to the language of pandemics, especially since words and imagery such as "viruses", "immunisation", "cyberhygiene" and others are already a core part of the cybersecurity lexicon. If so, then we may consider the individual user as a "disease" vector, as well as consider healthcare-related remedies such as mandatory vaccines and even quarantines.

To be responsible residents and guests in cyberspace, individual users require some basic literacy around cybertechnologies, cyberspace, and cybersecurity, just as basic literacy in hygiene is required to be a responsible citizen of a society, even more so during a pandemic (and the sheer volume of daily cyberattacks support the view that a cyber pandemic persists). If an individual does not understand the implications and applications of disclosing and distributing their personal information, then they have not properly consented to its use (Jaworska 2017, McManus et al. 2005). Given how revealing online patterns of behaviour can be (Henschke 2017b, Solove 2008), there is a need for special care in limiting what vulnerable and uninformed people do in cyberspace, and in educating them in the risks and hazards online. Such cyberliteracy is a broad social issue, and we can argue that a state has a duty to ensure that its citizens

are properly educated in both cybersecurity and in practical aspects of cyberspace more generally.

In this public health frame, certain countermeasures now might look more palatable. For instance, many cyberattacks are conducted via bot networks (or botnets), in which a small army of compromised computers or cyberenabled 'smart' devices (zombies), with unsuspecting owners, are unleashed upon a target like a mindless horde. This is generally how a distributed denial of service (DDoS) cyberattack works: to flood a site with so many requests that it seizes up. In other frames, it may seem unethical to hack back on these zombie computers, because they seem to be innocent here: the owners didn't know their machines have been infected and hijacked for bad purposes, so disabling or otherwise manipulating their machines without permission seems harmful to the innocent. But in the considered frame, perhaps whatever harm falls on these owners can be justified by the greater good of public health.

We need not "blame" owners for being infected, though many could be blameworthy for being careless or ignorant of basic cybersecurity. Regardless, an infected patient, whether innocent or not, must be addressed, and public health emergencies allow for forcible vaccination (e.g., installing a software patch on a zombie computer without the owner's consent) and even more dramatic measures equivalent to forced quarantines (e.g., "bricking" or entirely disabling a computer; zombies usually get killed in the movies, even if they used to be friends or family). This is to say that attribution might not matter as much as previously believed if what we care about are infections and not innocence. Relatedly, where societies can require education and training for activities that threaten public health, such as driving, it might not be so ridiculous to require computer training, since the damage one computer can do is arguably much greater than what one car can do.

Further to this, we need to ensure that those writing, applying and enforcing laws about cyberspace have an understanding of the reality of the risks and threats and implications of laws, policies, and strategies around cybersecurity. This take on technical literacy is a recognised problem in intelligence oversight. Due to the fact that "it takes years to understand the technicalities of intelligence, [term limits on oversight committees] resulted in limited and superficial knowledge of the technicalities with intelligence oversight" (Lester 2016, 15). The suggestion here is that cybersecurity and cyberspace policy development and legal drafting, implementation and enforcement face similar, if not worse, problems arising from a lack of necessary literacy.

Bringing the discussion full circle, the range of harms plays a role in responding to cybersecurity failures. Identity theft, for instance, can lead to economic harms as well

as social or psychological harms. Note that the effectiveness of responses to the different harms differ: economic harms are somewhat easy to reconcile, since if $1,000 is stolen from a bank account, it is relatively easy to replace that with an alternate $1,000. In contrast, if a person's virtual identity is hacked, wiped, or hijacked, it is much harder to offer compensation for that loss.

Parallel to this is an issue of equivalence of impacts and generational differences, as the emergence and dominance of cyberspace in the personal and social realm is a relatively recent phenomenon whose impacts may more significantly affect recent generations than older ones. Those who were born and grew up prior to cyberspace's infiltration of social lives are differently susceptible to harms than those who are "digital natives." A cybersecurity attack that brings down Facebook or Twitter could be seen by some as a good thing, but for those whose entire social lives and personal histories are psychologically tied to Facebook or Twitter, such an attack would be not merely an inconvenience but could pose ethically significant psychological harm (Canetti, Gross, and Manor-Waismel 2016).

Having moved from the international realm to state–state, to state–citizen, to the individual, we can find some firm footing for ethics in cybersecurity. If people suffer, if core protections like privacy or informed consent are violated, then, like all other areas of human interaction, these actions should be considered ethically problematic. Moreover, the significance of these harms and wrongs could be experienced differentially.

Emerging Technologies for Critical Infrastructure

In this section, we will briefly list a set of new technologies and practices that are being integrated into and developed for enhancing critical infrastructure that bring with them a range of particular ethical challenges. First is artificial intelligence (AI). While there are a range of technologies that AI can refer to, two key features are: that AI can be used to analyse large amounts of data at speeds that humans simply cannot do; and that AI can be used to either support human decision making or in fact make decisions in place of humans. With the first feature, we are increasingly seeing the problem of biases in AI (Buolamwini and Gebru 2018, Jiang and Nachum 2020, Binns 2018). This could be because of the design of algorithms in which the designer's biases are actively or implicitly designed in. Or it could be because the data sets that machine learning (ML) relies on are biased to begin with (Garvie 2019). The ethical problem with biases in AI is that these biases can be expressed in ways that perpetuate existing social and

personal biases (Garvie, Bedoya, and Frankle 2016) and can occur in ways that are opaque to the operators and subjects of the AI's decisions (Robbins 2019, 498). When used in a context like criminal justice, this raises even more ethical concerns about justice, fairness, and the legitimacy of criminal justice processes (Henschke 2020a, Garvie, Bedoya, and Frankle 2016).

This is not only a problem in terms of exacerbating and entrenching existing biases, it raises further issues of justice. As stated throughout this report, one of the key aspects of liberal democracies is that people are owed reasons for why certain decisions were made. AI complicates this because certain AI decisions are inexplicable – not even the designers of a particular ML application necessarily know how that ML processes the data, and they cannot explain how a particular outcome was reached. This means that those who use the given application or are subject to its outcomes lack the opportunity for those decisions to be explained to them. The suggestion here is that for key moral social or politically important services, perhaps inexplicable AI should not be used (Robbins 2019).

Following from this, a further necessity of justice in liberal democracies is the right of people to appeal a decision. For instance, what can an individual do if an AI-assisted decision is made that is problematic or detrimental to them? The recent Australian government experience with the "robodebt" program is one example of how automated decision making can not only be extremely stressful for those subject to such decisions, but it can potentially be illegal and ultimately against the government's own interests. The issue of explicability makes appeals harder, as it can be very hard to appeal a decision when no one knows how or why the decision was made. Any such right of appeal needs to be easily accessible, easily understood and timely. This is what some describe as algorithmic recourse: "the systematic process of reversing unfavourable decisions by algorithms and bureaucracies across a range of … scenarios" (Venkatasubramanian and Alfano 2020) .

AI often has to make deductions or inferences from limited information. A person's address, GPS movements, motor vehicle, and other data could be used to deduce that person's gender, ethnicity, economic class, religion, political affiliation, whether they might be an alcoholic or looking for an abortion, as well as other personal and sensitive information (Henschke 2017b). Some of those deductions might be illegal to use in considering a job or housing applicant, for example.

A related issue with AI is asking if there are particular sorts of decisions that AI should not make. This might be a combination of the process and type of decision being made – if the AI decision making process cannot be explained, then it fails a basic

requirement of political justice. Thus, areas exist where an individual's moral, social, political or legal rights might need to be protected from inexplicable AI decisions (Robbins 2019). A further idea is that some decisions are too ethically important to be left up to AI. The use of AI in lethal weapons to target and kill people, for instance, for some people is deeply morally problematic (Purves, Jenkins, and Strawser 2015). This view holds that such ethically significant decisions should only be the province of moral agents like humans.

Finally, the speed at which AI moves can become an issue. In cybersecurity, autonomous cyber defences as well as offences are conducted at digital speeds that human supervisors cannot keep up with. So, if AI were to take a serious action, such as to shut down an intranet or disable an attacker's computer, a lack of "meaningful human control" – a linchpin issue in the ethics debate about lethal autonomous weapons or "killer robots" (Roff and Moyes 2016) – could mean a responsibility gap, if errors and unintended harms were to occur.

Quantum computing is often touted as the next step in technological evolution and for some promises a range of opportunities "[T]hese new computers will bolster national security, accelerate scientific innovation, and boost computational power" (Humble and DeBenedictis 2019). While many of the ethical issues with quantum computing are likely just extensions of long running discussions in computer ethics (Floridi 2010), quantum's impact on encryption brings with it a set of particular ethical issues. People claim that quantum computing will be able to crack any and all traditional encryption methods (Möller and Vuik 2017). This will leave all communications, internet-connected data storage and even top-secret information potentially vulnerable to hacking and exfiltration. As discussed above, encryption may be a vital aspect of political freedom. Moreover, state security agencies require encryption for the safety of their own operations.

At the same time, quantum encryption presents a tool that might allow for uncrackable encryption (Bhatt and Sharma 2019, Denning 2019). The ethical issues here may not only be ones of the destruction of people's right to privacy and assumptions of anonymity, but they could also be ones of fairness. If quantum encryption is the only way to protect the content of one's communications, then only those with the resources and technological understanding will have access to encrypted communications. Quantum computing thus brings with it a range of ethical concerns arising from its ability to change how encryption works and who has access to it.

A third set of technologies that are currently revolutionising critical infrastructure is the development cyber-enabled physical systems: the 'Internet of Things' (IoT). "The

IoT refers to a complex network of interactive and technical components clustered around three key elements: sensors, informational processors, and actuators" (Allhoff and Henschke 2018, 55). The IoT raises a range of unique ethical issues as it is both an informational tool and a physical one (Henschke 2017c). The sensors and informational processors gather and communicate information, while the informational processors and actuators bring about physical changes in the world. This combination of capacities, coupled with the integration of connected smart devices into our homes, workplaces and lives mean that the IoT will provide a background "smart environment" that will be largely invisible to us. We often will not know which things in the world are gathering information on us or how that information will be shared, and will probably be unable to easily change how IoT-based decisions express themselves in the physical world.

These unique attributes suggest that there are five key areas where ethical issues may arise – informed consent, privacy, information security, physical safety and trust (Allhoff and Henschke 2018). Adding further complexity to these discussions is the fact that, due to the connected nature of the IoT, these issues often affect each other. If "informed consent is not properly tended to, risks abound with regards to privacy or information security. If privacy and information security are not properly tended to, risks abound with regards to physical safety. If anything is not properly tended to, risks abound with regards to trust" (Allhoff and Henschke 2018). The point here is not to offer solutions about ethics and IoT, but to point out that there are a range of emerging ethical issues with the IoT and that they require focused analysis, carried out in a way that does not lose sight of the complex interactions between different values.

One example of the ethical challenges arising in cyber enabled physical systems is the development of autonomous vehicles and autonomous vehicle systems. "[T]he main points of discussion are about safety, and associated issues of responsibility and agency… The approaches cover points like whether a non-human should have the capacity to kill a human… [and] whether a non-human is an agent in the relevant sense" (Henschke 2020c). Sven Nyholm's articles give an excellent overview of many of these ethical issues (Nyholm 2018a, b).

One area that needs closer scrutiny however is the need to recognise that an ethical analysis of autonomous vehicles cannot just consider the values designed into individual vehicles. We also have to consider autonomous vehicles as critical infrastructure at the level of a *system* (Borenstein, Herkert, and Miller 2017, Henschke 2020c). "This is because driving is a complex system. It involves a series of actors, parts, rules and institutions for it to operate effectively. If, for example, it turned out that there was no way to prosecute and punish those drivers who disobeyed the law because of

some problem with the police and the courts, then this would have impacts on how people drive… By [Autonomous Driving Systems] ADSs then [we] mean the complex socio-technical systems of driving that includes autonomous vehicles but is not limited to them. In addition to the interactions between autonomous vehicle, driver and other autonomous vehicles, the notion of ADSs deliberately includes the full range of road users" (Henschke 2020c). The point here is that effective accountability and oversight of the whole ADS is needed to ensure they are ethically justifiable but also trustworthy and usable.

Ethical Solutions: Putting Ethics into Practice

The final section provides guidance in how to effectively operationalise these ethical values into policies and practices. The report covers a very wide range of issues, each with their own complex sets of ethical discussions. While specific answers or guidance for each and every issue cannot be offered, the general notion of ethics as giving justificatory reasons is practically useful. What follows is a guide to help put ethical decision making into practice. Steps 2 – 8 are adapted from Michael Davis' chapter "Case Method", (Davis 1999).

1) *Clarify the concepts and values that you are working with.*

In the context of this report, the concepts that you are seeking to understand and the role of values are central. However, in order to make the role of these concepts and values both pragmatic and compelling, the key concepts must be identified, and the values specified and clarified. For instance, it is no good simply saying "we need people's behaviours in cyberspace to be ethical". The way you use concepts like cybersecurity, cyberspace, and critical infrastructure needs to be clarified and stated clearly. And the aspects of what makes behaviour 'good' need to be specified in relation to a given value or set of values, and those values need to be clarified. The tools to do this are provided in the early section of this report. You may also need to clarify specific concepts of relevance like "cyberattack" or "privacy" and give some reasons as to why you are using those concepts in the given way.

2) *State the problem*: For example, "there's something about this decision that makes me uncomfortable", or "there's a conflict of interest here" (Davis 1999).

The point of stating the problem is to clarify what exactly is causing the concern. It is not enough to simply say 'this is a problem'. You need to explain what the problem is. Issues in cyberspace can seem like they are ethical issues because this might be the first time you have encountered this issue.

3) *Check the facts*: Is this a real problem or are you confused about the facts? (Davis 1999)

A number of ethical issues in cyberspace may turn on the facts. For instance, you might be concerned about the privacy issues of a particular application, but perhaps

this application has no actual impact on privacy. Or, on the other hand, what may seem like a simple technical fix to an ongoing problem, like the need for backdoors into encrypted communications, might put the basic functioning of the internet at risk, so is far more of an issue than it first appears.

4) *Identify the relevant factors*: For example, are the people involved, any items or principles held to be important or sacred by a significant proportion of the relevant population? Are there laws, professional codes or other constraints that need to be considered? (Davis 1999)

This is essential to any ethical analysis of an issue – you need to be clear about who is affected by a particular decision, policy or application, how they are affected, what social norms, laws and other constraints are potentially going to be violated. For instance, as mentioned, many countries actively prohibit private citizens or institutions hacking back. Any actor that considers hacking back would need to be cognisant of the relevant laws that they might be breaking. In terms of particularly important items or principles, would the policy or decision degrade or offend some important object, symbol or ideal? The notion of critical infrastructure also becomes relevant here – if you are planning a particular cyberoperation, will this negatively impact the target's critical infrastructure, in what way, and who is likely to suffer and/or have their rights interfered with as a result?

5) *Develop a list of options*

This is an extension of the relevant factors – what are your options? What means do you have at your disposal, and who is best placed to pursue those means? (Davis 1999)

6) *Test options* (Davis 1999)

a) *Harms test*: does this option do more or less harm than others?

This draws from the basic notion of utilitarianism: that in order to know what you should do, you need to know what the harms of different options are. In a simple utilitarian calculation, you would take the option that causes the least amount of harm. As discussed earlier though, given that responses to cyberattacks may occur in cyberspace or the physical realm, there is a challenge in how you weigh up different sorts of harm.

b) *Rights test*: are there specific rights that are violated by acting, or do you have a duty to intervene to protect specific rights?

This draws from the basic idea of human rights: in order to know what you should do, you need to take into account the rights of others, whether your actions would violate those rights, and/or whether you have a special obligation to intervene to protect others' rights from being violated. This would probably run parallel to a legal analysis: are there legal rights that are being violated by a particular action, and/or does your institution or department have a special responsibility to protect particular rights from attack? Bear in mind, however, that these tests are going to be heavily influenced by how you and your institution think of moral, social, political, and legal rights.

c) *Reversibility test*: would you still think this was a good option if you or someone you care about was adversely affected by it?

This test goes to issues of fairness – if you would be unwilling to endure the outcomes, or if you would be unwilling to have those who you care about endure the outcomes, then it is likely that this option fails a basic test of fairness.

d) *Publicity test*: would you want your choice of this option published in the newspaper?

e) *Defensibility test*: could you defend your reasoning when under professional scrutiny?

Steps 6d and 6e are quite similar. They both rely on the notion of being able to give justificatory reasons. What they ask of you is to first reflect on those reasons, then to consider whether you would be willing to stand by those reasons in public. This is not a foolproof way of ensuring that one's justificatory reasoning is as good as it could be, but it does give one way to reflect on those justifications. Importantly, if you are worried about those reasons going public, and/or would not be willing to stand by those reasons in public, this should give you pause to reconsider your reasoning, which options you are considering, and why.

f) *Colleague test*: what do your colleagues say when you tell them about your problem and proposed solution?

If, for example, your colleagues were to be significantly worried about a particular option, it is a good sign that that option needs to be rethought. However, many institutions develop an institutional culture and can develop very similar values and ways of thinking. This is why one must also consider what the public at large would say about this option.

g) *Professional test*: what might your profession's governing body say about this?

h) *Organisation test*: what does your institution's legal officer say about this?

Steps 6g and 6h are quite similar. They are ways of using your institutional knowledge and expertise to test the options. They draw from the experience and moral authority of your professional bodies and the legal authority of the legal officer. However, as noted earlier in this report, what is legal is not necessarily ethical.

7) Make a choice and act

This is obvious, but needs to be stated. You cannot spend all your time reflecting on what to do and not actually do anything. For those in leadership positions, "no decision" can be a decision in and of itself.

8) Review steps 1 - 7

This review step is a fundamental aspect of reflection, to see what can be learnt from the given experience, what could be done better, what went wrong and why. Ethics here, as reasons that explain judgments then becomes woven into the reflection process as well. Ultimately this ongoing and evolving reflection process should not only produce better outcomes, but a more nuanced and effective ethics.

Bibliography

Allhoff, Fritz, Nicholas G. Evan, and Adam Henschke, eds. 2013. *Routledge Handbook Of Ethics And War: Just War In The 21st Century*: Routledge.

Allhoff, Fritz, and Adam Henschke. 2018. "The Internet Of Things: Foundational Ethical Issues." *Internet Of Things* 1-2:55-66. doi: https://doi.org/10.1016/j.iot.2018.08.005.

Allhoff, Fritz, Adam Henschke, and Bradley Jay Strawser, eds. 2016. *Binary Bullets: The Ethics Of Cyberwarfare*: Oxford University Press.

Altman, Andrew, and Christopher Heath Wellman. 2009. *A Liberal Theory Of International Justice*. Oxford: Oxford University Press.

Bhatt, Alekha Parimal, and Anand Sharma. 2019. "Quantum Cryptography For Internet Of Things Security." *Journal of Electronic Science and Technology* 17 (3):213-220. doi: https://doi.org/10.11989/JEST.1674-862X.90523016.

Binns, Reuben 2018. "Fairness In Machine Learning: Lessons From Political Philosophy." Proceedings Of The 1st Conference On Fairness, Accountability And Transparency, Proceedings Of Machine Learning Research.

Borenstein, Jason, Joseph R. Herkert, and Keith W. Miller. 2017. "Self-Driving Cars And Engineering Ethics: The Need For A System Level Analysis." *Science and Engineering Ethics*. doi: 10.1007/s11948-017-0006-0.

Bowden, Mark. 2011. *Worm: The First Digital War*. New York: Atlantic Monthly Press.

Brennan, Geoffrey, Lina Eriksson, Robert E. Goodin, and Nicholas Southwood. 2013. *Explaining Norms*. Oxford: Oxford University Press.

Buolamwini, Joy, and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities In Commercial Gender Classification." Conference On Fairness, Accountability And Transparency.

Canetti, Daphna, Michael L. Gross, and Israel Manor-Waismel. 2016. "Immune From Cyberfire? The Psychological And Physiological Effects Of Cyberwarfare." In *Binary Bullets: The Ethics Of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke and Bradley Jay Strawser, 157-176. Oxford University Press.

Ceva, Emanuela, and Michele Bocchiola. 2019. *Is Whistleblowing A Duty?* Cambridge: Polity Press.

Clapper, James R, and Trey Brown. 2019. *Facts And Fears*: Viking.

Coady, CAJ (Tony). 2008. *Morality And Political Violence*. Cambridge?: Cambridge University Press?

Coates, Tony J. 1997. *The Ethics Of War*: Manchester University Press.

Coleman, Stephen. 2013. *Military Ethics: An Introduction With Case Examples*. New York: Oxford University Press.

Comey, James. 2018. *A Higher Loyalty: Truth, Lies, And Leadership*. New York: Pan Macmillan.

Commonwealth Of Australia, Department Of Foreign Affairs And Trade. 2017. Australia's International Cyber Engagement Strategy.

Davis, Michael. 1999. *Ethics And The University*. London: Routledge.

Davis, Michael. 2005. "The Moral Justifiability Of Torture And Other Cruel, Inhuman, Or Degrading Treatment." *International Journal Of Applied Philosophy* 19 (2):161-178.

Delmas, Candice. 2015. "The Ethics Of Government Whistleblowing." *Social Theory And Practice* 41 (1):77 - 105. doi: DOI: 10.5840/soctheorpract20154114.

Denning, Dorothy E. 2019. "Is Quantum Computing A Cybersecurity Threat?" *American Scientist* 107 (2):83-85.

Floridi, Luciano, ed. 2010. *The Cambridge Handbook Of Information And Computer Ethics*. Cambridge: Cambridge University Press.

Forst, Rainer. 2012. *The Right To Justification: Elements Of A Constructivist Theory Of Justice*. New York: Columbia University Press.

Friedman, Batya, and David G Hendry. 2019. *Value Sensitive Design: Shaping Technology With Moral Imagination*. Cambridge: MIT Press.

Frischmann, Brett M. 2012. *Infrastructure: The Social Value Of Shared Resources*. Oxford: Oxford University Press.

Garvie, Clare. 2019. Garbage In, Garbage Out. Georgetown Center On Privacy & Technology.

Garvie, Clare, Alvaro Bedoya, and Jonathan Frankle. 2016. The Perpetual Line-Up: Unregulated Face Recognition In America. Washington DC: Georgetown Center On Privacy And Technology.

Glover, Jonathan. 2000. *Humanity : A Moral History Of The Twentieth Century*. New Haven, CT: Yale University Press.

Greenwald, Glen. 2014. *No Place To Hide: Edward Snowden, The NSA, And The U.S. Surveillance State*. New York: Metropolitan Books.

Haidt, Jonathan. 2012. *The Righteous Mind: Why Good People Are Divided By Politics And Religion*. London: Penguin.

Hayden, Michael V. 2019. *The Assault On Intelligence: American National Security In An Age Of Lies*. New York: Penguin Books.

Henschke, Adam. 2017a. "Duties To Defend: Ethical Challenges Of Cyberspace." In *Rethinking Security In The Twenty-First Century: A Reader*, edited by Edwin Daniel Jacob. Somerset: Palgrave Macmillan.

Henschke, Adam. 2017b. *Ethics In An Age Of Surveillance: Virtual Identities And Personal Information*. New York: Cambridge University Press.

Henschke, Adam. 2017c. "The Internet Of Things And Dual Layers Of Ethical Concern." In *Robot Ethics*, edited by Patrick Lin, Keith Abney and Ryan jenkins. Oxford: Oxford University Press.

Henschke, Adam. 2017d. "Weapons For Pacifism: Reconciling Ideas In Conflict." In *The Nature Of Peace And The Morality Of Armed Conflict*, edited by Florian Demont-Biaggi. London: Palgrave MacMillan.

Henschke, Adam. 2017e. "What Cyberweapons Tell Us About Our Just War." In *Ethics Under Fire*, edited by Tom Frame, 227-241. Sydney: UNSW Press.

Henschke, Adam. 2019. "Cybersecurity." In *International Encyclopedia Of Ethics*, edited by Hugh LaFollette, 1-8. Wiley.

Henschke, Adam. 2020a. "Information Technologies And Constructions Of Perpetrator Identities." In *The Routledge International Handbook Of Perpetrator Studies*, edited by Susanne Knittel and Zachary Goldberg, 217-227. London: Routledge.

Henschke, Adam. 2020b. "Privacy, The Internet Of Things And State Surveillance - Handling Personal Information Within An Inhuman System." *Moral Philosophy And Politics* 7 (1):123-149.

Henschke, Adam. 2020c. "Trust And Resilient Autonomous Driving Systems." *Ethics And Information Technology* 22:81-92. doi: doi:10.1007/s10676-019-09517-y.

Henschke, Adam. 2020d. "Why Would I Be A Whistleblower?" *Ethics And International Affairs* 34 (1):97-109.

Henschke, Adam, Matthew Sussex, and Courteney O'Connor. 2020. "Countering Foreign Interference: Election Integrity Lessons For Liberal Democracies." *Journal Of Cyber Policy*:1-19. doi: 10.1080/23738871.2020.1797136.

Hinduja, Sameer, and Justin W. Patchin. 2019. "Connecting Adolescent Suicide To The Severity Of Bullying And Cyberbullying." *Journal Of School Violence* 18 (3):333-346. doi: 10.1080/15388220.2018.1492417.

Humble, Travis S., and Erik P. DeBenedictis. 2019. "Quantum Realism." *Computer* 52 (6):13-17. doi: 10.1109/MC.2019.2908512.

Inness, Julie C. 1992. *Privacy, Intimacy, And Isolation*. New York: Oxford University Press.

Jaworska, Agnieszka. 2017. Advance Directives And Substitute Decision-Making. In *The Stanford Encyclopedia Of Philosophy* https://plato.stanford.edu/archives/sum2017/entries/advance-directives/, edited by Edward N Zalta.

Jiang, Heinrich , and Ofir Nachum. 2020. "Identifying And Correcting Label Bias In Machine Learning." Proceedings Of The Twenty Third International Conference On Artificial Intelligence And Statistics, Proceedings of Machine Learning Research.

Kaska, Kadri, Henrik Beckvard, and Tomas Minarik. 2019. "Huawei, 5G And China As A Security Threat." *NATO Cooperative Cyber Defence Center For Excellence (CCDCOE)* 28.

Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Skorvanek, Tomislav Chokrevski, and Masa Galic. 2016. "A Typology Of Privacy." *University Of Pennsylvania Journal Of International Law* 38:483.

Langner, Ralph. 2013. To Kill A Centrifuge: A Technical Analysis Of What Stuxnet's Creators Wanted To Achieve. Arlington: The Langner Group.

Lester, Geneveive. 2016. *When Should State Secrets Stay Secret?* Cambridge: Cambridge University Press.

Lin, Patrick. 2016. Ethics Of Hacking Back: Six Arguments From Armed Conflict To Zombies San Luis Obispo: National Science Foundation

Lucas Jnr, George R. 2016a. "Emerging Norms For Cyberwarfare." In *Binary Bullets: The Ethics Of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke and Bradley Jay Strawser. Oxford University Press.

Lucas Jnr, George R. 2016b. *Ethics And Cyber Warfare: The Quest For Responsible Security In The Age Of Digital Warfare*: Oxford University Press USA.

Macnish, Kevin. 2018. "Government Surveillance And Why Defining Privacy Matters In A Post-Snowden World." *Journal Of Applied Philosophy* 35 (2):417-432.

Manjikian, Mary. 2017. *Cybersecurity Ethics: An Introduction*. London: Routledge.

May, Larry. 2007. *War Crimes And Just War*. New York: Cambridge University Press.

May, Larry. 2008. "The Principle Of Just Cause." In *War: Essays In Political Philosophy*, edited by Larry May, 49-66. New York: Cambridge University Press.

May, Larry. 2012. *After War Ends: A Philosophical Perspective*. New York: Cambridge.

McMahan, Jeff. 2009. *Killing In War*. Oxford: Clarendon Press.

McManus, John, Sumeru G Mehta, Annette R McClinton, Robert A De Lorenzo, and Toney W Baskin. 2005. "Informed Consent And Ethical Issues In Military Medical Research." *Academic Emergency Medicine* 12 (11):1120-1126. doi: doi:10.1197/j.aem.2005.05.037.

Möller, Matthias, and Cornelis Vuik. 2017. "On The Impact Of Quantum Computing Technology On Future Developments In High-Performance Scientific Computing." *Ethics And Information Technology* 19 (4):253-269. doi: 10.1007/s10676-017-9438-0.

Mueller, Robert S. 2018. United States Of America V. Internet Research Agency. edited by United States Department Of Justice. District Of Columbia.

Muthuppalaniappan, Menaka, and Kerrie Stevenson. 2020. "Healthcare Cyber-Attacks And The Covid-19 Pandemic: An Urgent Threat To Global Health." *International Journal For Quality In Health Care* Online First. doi: 10.1093/intqhc/mzaa117.

Nickel, James. 2019. "Human Rights." accessed 10/04/2020. https://plato.stanford.edu/archives/sum2019/entries/rights-human/.

Nissenbaum, Helen. 2009. *Privacy In Context: Technology, Policy, And The Integrity Of Social Life*: Stanford Law Books.
Nyholm, Sven. 2018a. "The Ethics Of Crashes With Self-Driving Cars: A Roadmap, I." *Philosophy Compass* 13 (7):e12507. doi: doi:10.1111/phc3.12507.
Nyholm, Sven. 2018b. "The Ethics Of Crashes With Self-Driving Cars: A Roadmap, II." *Philosophy Compass* 13 (7):e12506. doi: doi:10.1111/phc3.12506.
Orend, Brian. 2013. *The Ethics Of War*. 2nd ed. Vancouver: University Of Alberta.
Purves, Duncan, Ryan Jenkins, and Bradley J. Strawser. 2015. "Autonomous Machines, Moral Judgment, And Acting For The Right Reasons." *Ethical Theory And Moral Practice* 18 (4):851-872. doi: 10.1007/s10677-015-9563-y.
Reglitz, Merten. 2019. "The Human Right To Free Internet Access." *Journal Of Applied Philosophy* 37 (2):314-331. doi: 10.1111/japp.12395.
Rid, Thomas. 2013. *Cyber War Will Not Take Place*: Hurst & Company.
Rid, Thomas. 2020. *Active Measures: The Secret History Of Disinformation And Political Warfare*. London: Farrar, Straus and Giroux.
Robbins, Scott. 2019. "A Misdirected Principle With A Catch: Explicability For AI." *Minds And Machines* 29 (4):495-514. doi: 10.1007/s11023-019-09509-3.
Robbins, Scott, and Adam Henschke. 2017. "Designing For Democracy: Bulk Data And Authoritarianism." *Surveillance And Society* 15 (3):582 - 589.
Roff, Heather, and Richard Moyes. 2016. Meaningful Human Control, Artificial Intelligence And Autonomous Weapons: Briefing Paper For UN CCW Meeting Of Experts On LAWS. Geneva: Article 36.
Ruys, Tom. 2010. Armed Attack And Article 51 Of The Un Charter: Evolutions In Customary Law And Practice. Cambridge: Cambridge University Press.
Schmitt, Michael N. 2011. "Cyber Operations And The Jus Ad Bellum Revisited." *Villanova Law Review* 56 (3):569 - 606. doi: https://ssrn.com/abstract=2184850.
Schmitt, Michael N., ed. 2013. *Tallinn Manual On The International Law Applicable To Cyber Warfare*: Cambridge.
Schmitt, Michael N., and Liis Vihul. 2016. "The Emergence Of International Legal Norms For Cyberconflict." In *Binary Bullets: The Ethics Of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke and Bradley Jay Strawser. Oxford University Press.
Schmitt, Michael N., and Liis Vihul, eds. 2017. *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*: Cambridge University Press.
Shue, Henry. 2020. *Basic Rights: Subsistence, Affluence, And US Foreign Policy*. 3rd ed. Princeton: Princeton University Press.
Smith, Michael. 1987. "The Humean Theory Of Motivation." *Mind* 96 (381):36-61.
Smith, Michael. 1994. *The Moral Problem*. Malden: Blackwell Publishing.
Solove, Daniel. 2008. *Understanding Privacy*. Harvard: Harvard University Press.
Solove, Daniel. 2013. *Security And Privacy*.
Steinhoff, Uwe. 2007. *On The Ethics Of War And Terrorism*: Oxford University Press.
Sussman, David. 2005. "What's Wrong With Torture?" *Philosophy And Public Affairs* 33 (1):1-33.
Thakur, Ramesh. 2016. "The Responsibility To Protect At 15." *International Affairs* 92 (2):415-434. doi: 10.1111/1468-2346.12557.
Venkatasubramanian, Suresh, and Mark Alfano. 2020. "The Philosophical Basis Of Algorithmic Recourse." Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, Barcelona, Spain.
Walzer, Michael. 2006. *Just War And Unjust Wars*. 4th ed. New York: Basic Books.
Wenar, Leif. 2020. "Rights." accessed 10/04/2020. https://plato.stanford.edu/archives/spr2020/entries/rights/.
Zuboff, Shoshana. 2019. *The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power*. London: Public Affairs.

Published by
Conflict Studies Research Centre

Editor: Keir Giles

ISBN 978-1-908428-14-1