Exploring the ethics of cyber deception technologies for defensive cyber deception

Iain Reid[1], Angela Okeke-Ramos[1] and Mikolaj Serafin[1]

[1] *University of Portsmouth, School of Criminology and Criminal Justice, High Street, Portsmouth, UK.*

Abstract

Cyber deception technologies are increasingly being deployed for defensive cyber deception, in protecting our computer networks from attack. Typically, these approaches have focused on conducting cyber deception for generating threat intelligence through studying attackers' tactics, techniques and procedures, alongside the potential for covert exfiltration of digital forensics related to the attacker. Some more recent research has sought to develop concepts related to oppositional human factors, which target attacker cognition, perception and decision-making. As cyber deception technologies seek to influence human cognition and behavior, this paper proposes that there are a number of ethical issues that need to be considered in their deployment, alongside a number of potential ethical justifications for the use of such technologies in defending organization's computer networks.

Keywords

Defensive Cyber Deception, Cyber Deception Technologies, Ethics

1. Introduction

Cyber deception technologies are both increasingly sophisticated and increasingly being integrated into Defensive Cyber Deception (DCD) to defend against computer network intruders. Cyber deception technologies are complex socio-technical systems, whereby software created by individuals and organizations, is used for deceptive reasons to influence computer network intruders, and, potentially the organizations they work for. Fugate and Ferguson-Walter (2019) outline how defenders are required to restrain responses to attackers due to ethical and legal principles, whilst attackers do not face this challenge [1]. This further exacerbates the asymmetric advantage of attackers against defenders. DCD tools and techniques seek to disrupt this asymmetric advantage held by cyber attackers and intruders through challenging attackers across the cyber to the cognitive battlespace [2]. Deception itself is defined as "deliberate measures to induce erroneous sensemaking and subsequent behavior within a target audience, to achieve and exploit an advantage" [3]. The key elements here are erroneous sensemaking, an intentional act to bring the deceiver an advantage, a focus on the process of induction used by the victim, causing a change in behavior, and targeting a specific audience [2]. Whilst such approaches have begun to address the balance of power between attacker and defender [1, 4, 5], there has been limited research into the ethical implications of DCD [6]. One of the most common reactions is that it would be unethical to do so, even if it is not always the case [7]. Furthermore, Ashenden et al. (2021) found that subject matter expert (SME) participants in their research believed organizations need to discuss the ethics and legalities of using cyber deception technologies to defend against attackers [2]. The aim of this position paper is to outline DCD, identify the ethical considerations of conducting DCD, alongside exploring potential ethical frameworks for conducting DCD drawing upon research related to the ethics of cybersecurity, military deception and cyberwarfare.

The 10th International Conference on Socio-Technical Perspectives in IS (STPIS'24) August 16-17 2024 Jönköping, Sweden

iain.reid@port.ac.uk (I. Reid); up2006788@myport.ac.uk (A. Okeke-Ramos); up2021237@myport.ac.uk (M. Serafin)

0000-0003-4072-7557 (Iain Reid)

2. Defensive Cyber Deception

In using DCD to protect computer networks, cyber deception technologies have traditionally focused on the use of honeypots, simulated computer networks, which seek to attract attackers away from the actual computer network [8, 9]. Once inside the honeypots, attacker's tactics, techniques and procedures (TTPs) are monitored to further understand, and potentially attribute, the attacker. The key purpose of honeypots is to generate threat intelligence, whereby network defenses can be further strengthened to increase cyber security. The further development of cyber deception technologies for DCD has moved beyond honeypots, however the premise of such technologies is still focused around studying attacker TTPs for generating threat intelligence. Some cyber deception technologies also enable the covert exfiltration of data regarding the data, moving beyond the studying of TTPs to potentially begin to attribute an attacker. Further research developing approaches to DCD has focused beyond threat intelligence and has sought to actively engage with attackers and to challenge them across the cyber and psychological battlespace [10, 11, 12, 13]. These approaches aim to cause uncertainty, confusion, surprise, selfdoubt and frustration in attackers, to slow down their attacks, and create surprise in the attackers [10, 11, 13]. The unknown here is whether such cyber deception causes any psychological harm to an attacker, or whether it is seen as merely an inconvenience and if the attacker will move on to an easier target. As both public and private organizations implement DCD measures there is a need to understand the ethical implications of these measures [6, 14], particularly where there may be suggestions of the development of more offensive responses [2]. Such offensive responses, including hack-back, are primarily located within the remit of nationstates and are not available to organizations that deploy DCD.

3. Ethical considerations

The limited research exploring the ethical considerations of conducting cyber deception has primarily sought to explore entrapment, privacy, and liability [6]. Predominantly this work has focused on the legal, rather than ethical considerations, and upon US legislation with a smaller amount on European legislation. The general conclusion of this work has argued that cyber deception is acceptable to be conducted by law enforcement and organizations in terms of selfdefense and reducing risk [6]. However, research exploring the ethical considerations of cyber deception remains limited [6].

The following sections draw upon the limited research into the ethics of cyber deception, alongside ethics of cybersecurity, the ethics of cyberwarfare and the ethics of military deception to explore potential ethical considerations of cyber deception technologies for DCD. Ethical issues in conducting DCD include: 1) issues associated with Internet safety and introducing vulnerabilities to the public; 2) the morality of making users part of an experiment without their awareness and consent; 3) the morality of enticing someone to commit a crime; 4) cyber perfidy; 5) responsibility and automation; and 6) the potential for harm to an attacker. Overall, there is a strong requirement to explore the issues surrounding the ethics of cyber deception, specifically as cyber deception technologies are being increasingly deployed by organizations to actively protect their computer systems from attackers.

3.1. Internet safety and introducing vulnerabilities to the public

A major consideration for the use of cyber deception technologies for DCD is that of Internet safety and introducing vulnerabilities to the public, including the potential for third party vulnerabilities [6, 14]. Potential vulnerabilities may be introduced to the public that cause unintentional harm to neutral or third parties, and associated with potential cascading effects, which has been a longstanding ethical consideration in cyberwarfare [15]. Expanding on the

concept of cyberwarfare immunity for all third-parties is required [16]. In applying such considerations to cyber deception technologies for DCD, such ethical considerations may not be required where deceptive assets are deployed within a network where legitimate users would not be accessing them. Furthermore, as the majority of current commercial-off-the-shelf (COTS) DCD solutions are for generating threat intelligence, as opposed to more offensive responses, then this ethical consideration may not need to be considered as in-depth with more potentially offensive responses. Alternatively, if COTS DCD solutions move beyond the current focus on generating threat intelligence and move towards more offensive responses then there will be a need to consider potential harm to neutral and third parties through cascading unintentional effects. Developing an understanding of any potential harms to neutral and third parties from DCD will be need to considered as part of wider DCD planning and lifecycle management.

3.2. The morality of making users part of an experiment without their awareness and consent

With the deployment of cyber deception technologies for DCD there are potential ethical issues related to the morality of making users of a system part of an experiment without their awareness and consent. For example, there are concerns about privacy when using fake login props, defensive phishing or social engineering [7]. While there is an argument to be made about ethical issues when collecting attacker's information without their consent [17], this is not usually an issue as attackers are typically anonymous when conducting illegal activities [7]. More recent cyber deception technologies for DCD do make claims for the covert exfiltration of digital forensics related to the attacker that can potentially be used for attribution, however, as these attackers are in breach of the Computer Misuse Act 1990 [18] these actions are arguably ethically justifiable.

Of more concern is the ethical issue regarding privacy in cyber deception is when a legitimate user encounters a cyber deception [7]. Since cyber deception should not target legitimate users, their data should be encrypted and deleted as soon as they are verified as legitimate users [7]. Therefore, there is some argument that cyber deception technologies should be made so that they have limited or no interactions with everyday users [7]. However, there is still an argument that cyber deception technologies for DCD should have deployment in parts of the network that legitimate users may use, as a specific strategy for targeting potential insider threats. Further, some cyber deception technology vendors have developed capabilities for deploying deception outside of the network (e.g. on GitHub) as a means of an early-warning system that an attack is occurring.

3.3. Entrapment

One potential ethical issue that may occur in the use of cyber deception technologies for DCD is entrapment [6, 7, 9]. Specifically, the use of honeytokens, honeyfiles, and honeypots can be potentially seen as entrapment [7, 9]. This is an ethical issue as entrapment can be considered as an encouragement for committing crimes that would not be committed otherwise [7]. On the other hand, entrapment can be considered as being passive and the attacker is the one that takes the active role in committing crime [7]. This demonstrates that it can be difficult to determine what is and is not ethical when using cyber deception techniques. Entrapment as an ethical issue for cyber deception technologies for DCD may not be applicable for all cyber deception tactics and strategies, as not all approaches utilize honey technologies to attract users into deceptive environments, for example, the use of deceptive signaling [19, 20].

3.4. Cyber perfidy

One potential ethical issue that has application from the physical world to the virtual world, is that of cyber perfidy. Perfidy itself is taken from physical warfare whereby combatants are

required to act in good faith [21]. For example, when an adversary surrenders they are not then harmed; or the use of false insignia to suggest they are actors from another nation, or to hide who they really are whilst harming others [22]. Perfidy as an ethical issue may have challenges in its application to cyberspace. In relation to cyber perfidy there is some discussion over using a neutral domain name or adversary insignia or signatures in pretending to be the enemy during a visible cyberattack, however, if an adversary is not killed, wounded or captured then this should not be considered as perfidy [23]. Further issues raised as to what happens if this attack is autonomous, or whether a system can recognize the emblems of an adversary in cyberspace [23]. Although using false credentials in a military cyberattack may be considered perfidious [23], of note is that the deception here is only considered in the arguments as part of an offensive cyber operation, rather than as part of DCD.

There are further assumptions that it is only military networks that are being targeted rather than civilian networks. [23] refers to use by the NSA and GCHQ of a deception technique where users were redirected to a honeypot before malicious code was then injected onto the user's computer. Although this may parallel similar approaches to DCD the aim here was to target specific users, and it is unclear whether this may be considered perfidious unless it causes death, injury or capture of an enemy. The focus on perfidy and the physical harm that may result from perfidious actions ignores any harms that may be considered psychological. [23] argues that the use of cyberweapons which damages physical or virtual infrastructure or corrupts data belonging to the military may be considered as a morally permissible cyberattack, even when using a trusted certificate, software exploit or unauthorized credential. However, even though such capabilities may be considered as permissible they are moving beyond the capabilities of COTS cyber deception technologies.

3.5. Responsibility and automation

With the use of cyber deception technologies for DCD there are ethical issues related as to who holds overall responsibility for the deception deployed, and how this may be impacted by the automation of responses. One argument suggests that the ethical responsibility for cyber deception lies with the software developers who create the deception technology itself [7, 9]. This is opposed to those who may actually plan the DCD, or those who order the procurement or deployment of COTS cyber deception technology across a system or network.

In assessing the ethical responsibility for DCD through applying concepts from cyberwarfare there is further support that those who create actions (whether attacks or exploits) should be those who are held ethically responsible for the outcomes of these [24]. However, due to limitations or biases in decision-making humans may not know the outcomes of such actions suggests that cyberattacks or exploits may have uncertain moral legitimacy [24]. Although there is an assumption here that a response to a cyberattack is being conducted by the 'human in the loop' rather than an autonomous response guided by AI and/or ML, as is the case with COTS cyber deception technologies.

3.6. The potential for harm to an attacker

One interesting ethical consideration for cyber deception technologies for DCD is to whether deceptive assets have the potential to cause harm to an attacker. Applying concepts from cyberwarfare it is not clear how an attack on a computer system or network may be conceptualized as leading to 'damage' or whether this has a psychological or physical impact on the target, or how they may perceive such 'damage' [24, 25, 26]. Dipert (2016) further argues that deception in cyberspace is not substantive compared to deception in warfare, and that ethical comparisons are difficult to justify where there are no intentional or negligent deaths or permanent destruction [25]. More recent research utilizing concepts from oppositional human factors (OHF) has found that some approached to DCD are able to cause confusion and surprise in attackers [10, 11, 13], however, it is again unclear as to whether this may translate into actual physical or psychological harm to an attacker.

In seeking to understand the psychological harms of cyberwarfare Canetti et al. (2016) extrapolate findings from research exploring the impact of more common online and offline harms [27]. Cyberoperations that target individuals, networks or facilities may not result in any suffering to an individual, and if non-combatants were targeted this would still not equate to cyberterrorism [27]. Victims of cyber-attacks in the form of identity theft have experienced psychological harm that is argued to be akin to that of burglary and home invasion, whilst being a victim of cyberbullying results in psychological trauma [27]. In an experimentational simulation of a cyberattack (an intrusive breach of privacy), Canetti et al. (2017) found that there was an increase in cortisol levels, which are indicative of a physiological response to stress [28]. Whilst Canetti et al. (2016) argue that as cyberattacks may cause such psychological and physiological harms then they should not be used against non-combatants as it is not morally acceptable [27]. However, if such attacks may be deployed against those who attack our computer networks then this would be considered acceptable. Further investigation is required to explore whether the use of cyber deception technologies for DCD, can lead to potential psychological or physiological harm to an attacker.

4. Ethical Frameworks

In seeking to establish ethical justifications for the deployment of cyber deception technologies for DCD this work again draws upon the existing research exploring the ethics of cyber deception, alongside that of the ethics of cyber security, cyberwarfare and military deception. This work proposes that there are a number of potential ethical justifications that can be used for the support of the use of cyber deception technologies in DCD, considering cyber deception for threat intelligence, and the move to potential approaches for disrupting attacker cognition and decisionmaking. As Loi and Christen (2020) [29] highlight cyber security explicitly states its ethical goal of being free from harm or danger in cyberspace, however, the challenge is whether the means to ensure this security are ethical or not.

4.1. Principlist

The principlist framework of ethics is argued to be grounded in reality and professional ethical practice that enables flexibility in making decisions [29]. Principlism itself is a deontological perspective to moral rightness, whereby the ethics are through fulfilling the prima facie act even if this produces negative consequences [29]. There may be three or four moral principles that are regarded to as prima facie duties in the deployment of cyber deception technologies for DCD in defending organizations against attackers. These should be identified by the organization itself as the ethical principles that they wish to adhere to, with the acknowledgement that such principles may sometimes clash with one another.

4.2. Human Rights

There needs to be a balance of human rights and security in cyberspace, the challenge is in which context one or the other becomes the priority [29]. For example, as individuals we have the right to privacy, and cyber deception technologies for DCD may seek to enhance this through the use of the deployment of deceptive assets seeking to prevent cyberespionage or ransomware attacks that breach an individual's right to privacy. Rights associated with profiling and cyber security may not be applicable in the case of cyber deception, as if individuals are already intruding in our computer networks then they are already in breach of the Computer Misuse Act 1990 [18]. However, as cyber deception technologies for DCD may covertly extract digital forensics for threat intelligence then the potential for misattribution of an attacker also needs to be considered as an ethical issue.

4.3. Proportionality

Across the existing literature on the ethics of cyberwarfare and cyberdefense for organizations there is a consensus that a response to a cyberattack must be proportionate to the magnitude and scope of the provocation [14, 16, 24]. This includes the fact that there should be no overreaction of acts of vigilantism [14, 16] or impact on third parties [26], or on privacy [30]. The principle of proportionality may be applied to cyber deception technologies for DCD, for example, delays or tarpits are considered a cyber deception technique that is used to slow down an attacker, it has low impact on the legitimate users as attackers are usually in a more of a hurry [7, 17]. The main ethical issue regarding the use of tarpits is if the network decides to delay the network long after the attacker is gone in anticipation of another attack.

Stevens (2020) argues that measures by organizations should be viewed in terms of subsidiarity and proportionality [14]. With the case of subsidiarity, the measures used to avert a cyberattack may be considered ethically justified when the threat could not have been averted or minimized using a less invasive measure, or applied in a less invasive measure [14]. In terms of proportionality, this would be argued to maintain a balance between the imminent harm avoided by an organization against harm to an innocent third party or even potentially an attacker [14]. Stevens (2020) argues that in calculating the parameters of a defensive measure than there is a need to foresee the consequences of our actions alongside the harms averted to a degree of reasonable certainty [14].

As the key of focus of currently available COTS cyber deception technologies for DCD is on generating threat intelligence, then the use of deceptive assets overall may be considered as a proportional response to a cyberattack. The potential harm posed by the use of cyber deception assets is beneath that of the harm posed by an attacker to an organization, whether they are conducting cyberespionage, or seeking to inject ransomware into a network.

4.4. Self-defense

Expanding on the ethics of cybersecurity to how organizations may ethically conduct DCD, Stevens (2020) explores the right to self-defense in cyberspace as ethical justification for specific cy-berdefense measures [14]. Stevens (2020) classifies measures that includes deception as potentially ethically problematic depending on their application [14]. Some measures may be considered as acts of cybervigilantism if an attack has finished and the action may be considered as punishment or having a retaliatory nature then they may not be ethically justified if conducted by a private organization as opposed to a law enforcement agency [14]. However, such arguments may not be applicable to DCD, whereby deceptive assets are utilized during an attack, whilst covert exfiltration of digital forensics may not be considered as an act of cybervigilantism.

In warfare self-defense is linked to liability to harm an attacker, where there is a necessity to harm an attacker to achieve a justifiable goal, and such responses should never knowingly inflict disproportionate harm to an attacker [31]. Adapting Jenkins (2016) [31] discussion of cyberwarfare as ideal war, if defenders incorporate cyberweapons into cyber deception technologies against attackers then this could be considered as ethically justified if the response is proportionate and there is no risk to non-combatants, although such an argument is currently theoretical. A point to consider here is that DCD efforts, to date, have sought to generate threat intelligence and disrupt attacker decision-making rather than, for example, encourage them to download a document that may include malware. The debate here is how harm to the attacker may be considered, and what ethics may relate to causing changes in an attacker's cognition through cyber deception. A further point Jenkins (2016) raises with offensive cyber operations is how far operations should be aimed downstream to focus on targets that will enable the desired effects to be achieved [31]. Applying this concept to DCD it brings about the question of who the defender wishes to deceive, an attacker who may be conducting the attack on behalf of others, or whoever may have given the orders and instructions for an attack. The desired effects of the cyber deception may wish to focus on the decision-making beyond the initial attacker, and instead seek to disrupt those who may be running cyber-attacks.

5. Implications for Research and Practice

Whilst there has been limited research into the ethics of conducting cyber deception for DCD there are a number of potential areas that need to be further researched, particularly in relation to practice, and how organizations may ethically deploy cyber deception technologies. Firstly, research is needed to establish whether and how organizations, both public and private, consider ethical issues related to conducting DCD, and how they may justify the use or non-use of cyber deception technologies. It is anticipated here that there may be differences between private organizations who may primarily be utilizing DCD for threat intelligence, as opposed to public organizations who may wish to deploy OHF approaches to affect attacker decision-making, cognition and behavior. Secondly, it is important to establish whether OHF approaches may actually cause harm to an attacker, or if they are merely seen as an inconvenience or annoyance through their attempts to disrupt attacker decision-making, cognition and behavior. Establishing whether harm does occur or not may address the ethical issues of causing harm to an attacker, and resultantly the need for proportionality, and subsidiarity in responses against an attacker. Thirdly, if organizations are choosing to deploy cyber deception technologies for DCD, then there is a need to understand where and how they consider ethical issues and justifications as part of the cyber deception planning process and associated lifecycle management [32]. A potential overall outcome for practice of this work combined would be organizational guidelines and polices for the ethical implementation of cyber deception technology for DCD.

6. Discussion and Conclusion

Deception is itself is considered neutral [33], it is the manner in which cyber deception technologies for DCD are deployed and utilized which gives rise to potential ethical issues. Adapting ethical positions from cybersecurity and cyberwarfare has enabled an examination of the justifications for cyber deception to be conducted, focusing on both the principlist and human rights ethics frameworks are considered as non-utilitarian as they do not require acts to be defined as for the greater good, rather they take a more risk-based and pragmatic approach in seeking to conduct ethical behavior in using cyber deception technologies for DCD. It may be best left to an organization to define what their key principles of ethics are, and how they may best ethically deploy deceptive assets in the defense of their organization against attackers.

Developing further the ethical justifications of cyber deception technologies for DCD it can be considered that the use of deceptive assets is justified according to both proportionality and subsidiarity of the responses against computer network attackers. As current deceptive assets are primarily focused on conducting cyber deception for threat intelligence rather than more offensive measures, such deception may be considered as following the principles of proportionality and subsidiarity. In particular when following principles of self-defense, the use of cyber deception technologies for DCD by organizations is considered as ethically justified, as such deceptive assets are only designed to be only interacted by with computer network attackers

In conclusion, as deception is considered neutral, it may be considered acceptable to deceive in crisis situations, to an adversary, or when deception has been used against us [34]. A number of ethical theories have sought to be applied to cyberspace [9], however, these theories may have limited application regarding the ethics of DCD in general [6]. Rowe (2008) states that the most appropriate ethical theory to follow regarding the ethics of cyber deception is utilitarianism where the benefits are assessed according to the overall benefit to society [9]. This further develops the arguments of Rowe (2004) where deception may be considered ethical when the costs of no deception are dearer than the cost of using deception, and where our own deception rarely catches legitimate users [35].

References

[1] S. Fugate, K. Ferguson-Walter, Artificial intelligence and game theory models for defending critical networks with cyber deception, AI Magazine, 40 (2019) 49-62.
[2] D. Ashenden, R. Black, I. D. Reid, S. Henderson, Design thinking for cyber deception, in: Proceedings of the 54th Hawaii International Conference on System Sciences, 2021, pp. 1958-1967. URL: https://hdl.handle.net/10125/70853.
[3] S. M. Henderson, Deceptive Thinking, In: 1st MilDec Military Deception Symposium, 2011.
[4] K. J. Ferguson-Walter, D. S. LaFon, T. B. Shade, Friend or Faux: Deception for cyber defense. Journal of Information Warfare, 16 (2017) 28-42.
[5] R. S. Gutzwiller, S. M. Hunt, D. S. Lange, A task analysis towards characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts, in: 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), IEEE, 2016, pp. 14-20.
[6] D. Fraunholz, S. D., Anton, C., Lipps, D., Reti, D., Krohmer, F., Pohl, M., Tammen, H. D., Schotten, Demystifying deception technology: A survey, 2018, URL: https://arxiv.org/abs/1804.06196
[7] N. C. Rowe, J. Rrushi, Introduction to Cyberdeception, Springer International Publishing, 2016.
[8] F. Cohen, The deception toolkit, Risks Digest, 19 (1998).
[9] N. Rowe, The ethics of deception in cyberspace, in: R. Luppicini, R. Adell (Eds.), Handbook of Research on Technoethics, IGI Global, 2008, pp. 529-541.
[10] K. Ferguson-Walter, M. Major, D. Van Bruggen, S. Fugate, R. Gutzwiller, The world (of CTF) is not enough data: Lessons learned from a cyber deception experiment, in: IEEE 5th International Conference on Collaboration and Internet Computing (CIC), IEEE, 2019, pp. 346-353.
[11] K. J. Ferguson-Walter, R. S. Gutzwiller, D. D. Scott, C. J. Johnson, Oppositional Human Factors in Cybersecurity: A Preliminary Analysis of Affective States, in: 36th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW), IEEE/ACM, 2021, pp. 153-158.
[12] R. S. Gutzwiller, K. Ferguson-Walter, S. Fugate, A. Rogers, "Oh, Look, A Butterfly!" A Framework For Distracting Attackers To Improve Cyber Defense, In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 2018, pp. 272-276.
[13] T. B. Shade, A. V. Rogers, K. J. Ferguson-Walter, S. B. Elson, D. K. Fayette, K. E. Heckman, The Moonraker Study: An experimental evaluation of host-based deception, in: Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020, pp. 1875-1884. URL: https://hdl.handle.net/10125/63970
[14] S. Stevens, A framework for ethical cyber-defence for companies, in: M. Christen, B. Gordjin, M. Loi (Eds.), The Ethics of Cybersecurity, Springer Open, 2020, pp. 317-330
[15] P. Lushenko, Binary Bullets: The Ethics of Cyberwarfare, edited by Fitz Allhoff, Adam Henschke and Bradley Jay Strawser, Journal of Military Ethics, 15 (2016) 69–73.
[16] J. Arquilla, Twenty years of cyberwar, Journal of Military Ethics, 12 (2013) 80-87.
[17] L. Zobal, D. Kolář, R. Fujdiak, Current state of honeypots and deception strategies in cybersecurity, in: 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), IEEE, 2019, pp. 1-9.
[18] Computer Misuse Act 1990 c. 18. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents
[19] P. Aggarwal, E. A. Cranford, M. Tambe, C. Lebiere, C. Gonzalez, Deceptive signalling: Understanding human behaviour against signalling algorithms, in: T. Bao, M. Tambe, C. Wang (Eds.), Cyber Deception: Techniques, Strategies and Human Aspects. Springer, Cham, Switzerland, 2023, pp. 83-96.
[20] C. Lebiere, E. A. Cranford, P. Aggarwal, S. Cooney, M. Tambe, C. Gonzalez, Cognitive modelling for personalized, adaptive signalling for cyber deception, in: T. Bao, M. Tambe, C. Wang (Eds.), Cyber Deception: Techniques, Strategies and Human Aspects, Springer, Cham, Switzerland, 2023, pp. 59-82.
[21] S. Watts, Law-of-War Perfidy, Military Law Review, 219 (2014) 106-175.

[22] M. Robinson, K. Jones, H. Janicke, Cyber warfare: Issues and challenges, Computers & Security, 49 (2015) 70-94.
[23] H. M. Roff, Cyber perfidy, ruse, and deception, in: F. Allhoff, A. Henschke, B. J. Strawser (Eds.), Binary Bullets: The Ethics of Cyberwarfare, Oxford University Press, 2016, pp. 201-227.
[24] D. Danks, J. H. Danks, Beyond machines: Humans in cyberoperations, espionage, and conflict, in: F. Allhoff, A. Henschke, B. J. Strawser (Eds.), Binary Bullets: The Ethics of Cyberwarfare, Oxford University Press, 2016, pp. 177-197.
[25] R. R. Dipert, Distinctive ethical issues of cyberwarfare, in: F. Allhoff, A. Henschke, B. J. Strawser (Eds.), Binary Bullets: The Ethics of Cyberwarfare, Oxford University Press, 2016, pp. 56-72.
[26] S. Miller, Cyberattacks and "Dirty Hands": Cyberwar, cybercrime, or covert political action? in: F. Allhoff, A. Henschke, B. J. Strawser (Eds.), Binary Bulletts: The Ethics of Cyberwarfare, Oxford University Press, 2016, pp. 228-250.
[27] D. Canetti, M. L. Gross, I. Waismel-Manor, Immune from cyberfire? The psychological and physiological effects of cyberwarfare, in: F. Allhoff, A. Henschke, B. J. Strawser (Eds.), Binary Bullets: The Ethics of Cyberwarfare, Oxford University Press, 2016, pp. 157-176.
[28] D. Canetti, M. Gross, I. Waismel-Manor, A. Levanon, H. Cohen, How cyberattacks terrorize: Cortisol and personal insecurity jump in the wake of cyberattacks, Cyberpsychology, Behavior and Social Networking, 20 (2017) 72-77.
[29] M. Loi, M. Christen, Ethical frameworks for cybersecurity in: M. Christen, B. Gordjin, M. Loi (Eds.), The Ethics of Cybersecurity, Springer Open, 2020, pp. 73-95.
[30] J. S. Hempson-Jones, The ethics of online military information activities, Journal of Military Ethics, 17 (2018) 211-223.
[31] R. Jenkins, Cyberwarfare as ideal war, in: F. Allhoff, A. Henschke, B. J. Strawser (Eds.), Binary Bullets: The Ethics of Cyberwarfare, Oxford University Press, 2016, pp. 89-114.
[32] K. E. Heckman, F. J. Stech, R. K. Thomas, B. Schmoker, A. W. Tsow, Cyber Denial, Deception and Counter Deception: A Framework for Supporting Active Cyberdefense, Springer, 2015. [33] S. Henderson, Creativity and morality in deception in: H. Kapoor, J. C. Kaufman (Eds.), Creativity and Morality, Academic Press, 2023, pp. 101-124.
[34] N. Rowe, Counterplanning deceptions to foil cyber-attack plans, in: IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, IEEE, 2003, pp. 203-210.
[35] N. Rowe, A model of deception during cyber-attacks on information systems, in: IEEE First Symposium on Multi-Agent Security and Survivability, IEEE, 2004. pp. 21-30.