Pandemic Speed: Accelerating Innovation in Cyber Security

Ian Wiltshire, Sujana Adapa, and David Paul

Introduction and Background

It would be difficult to miss the multitude of cybercrime reports that have appeared in general news over the past few years. In May 2021, the US oil delivery network run by Colonia Pipeline (Turton & Mehotra, 2021), suffered a cyberattack that caused operations to cease for several days. In June 2021, meat supplier JBS was effectively shut down for five days following a cyberattack which disabled its processing operations (Claughton & Beilharz, 2021). In July 2021, Microsoft's Exchange Server software was found to be compromised and NSW Department of Education was forced to take internal systems offline (NSW Government, 2021). Modern day cyberattacks now have the ability to cause substantial

I. Wiltshire · S. Adapa (✉) · D. Paul
University of New England, Armidale, NSW, Australia
e-mail: sadapa2@une.edu.au

I. Wiltshire
e-mail: iwiltshi@myune.edu.au

D. Paul
e-mail: dpaul4@une.edu.au

S. Adapa et al. (eds.), *Small and Medium-sized Enterprises, and Business Uncertainty*, Palgrave Studies in Global Entrepreneurship,
https://doi.org/10.1007/978-981-99-4844-4_9

damage to industry with their destruction and damage of data, process and physical hardware. Overall, cybercrime appears to be increasing in both the variety of victims and the number of attacks.

Distributed Denial of Service (DDoS) attacks as an attack method have also seen a drastic rise in prominence over the last few years (Bhattacharyya & Kalita, 2016; Cook, 2021; Nicholson, 2021), highlighted by the recent large and impactful attacks such as Google in 2017 (Nicholson, 2021), Git Hub in 2018 (Chadd, 2018; Newman, 2018) and AWS in 2020 (Crane, 2020).

These attacks were notable due to their large volume but DDoS does not just rely on flooding internet pipes with high bandwidth attacks to succeed. Sophisticated DDoS attack methods can also target internal server resources, aimed at depleting functional capabilities by using methods such as amplification and malformed requests (Alyas et al., 2017; Ismail et al., 2021). The goal is the same but, whilst volumetric attacks can be easily discovered by a sudden tidal wave of data flooding in, sophisticated attacks may use a slow trickle of requests to services that take some time to complete. This way, sophisticated attacks can cause system bottlenecks and slowly strangle the service until it eventually fails (Alyas et al., 2017).

Along with their scale, the three DDoS attacks noted above were also notable due to the target being well-known organisations, however, data from sources such as Akamai suggests that target sectors are now much more evenly spread (Akamai, 2020) when compared to attacks between 2016 and 2018 (Akamai, 2016), where vandalism and gaming were the primary target (Arbor, 2018). All industry sectors may now present an equally valid target for attacker at any scale.

DDoS attacks operate differently to other forms of cyberattack as the attacker does not need to find a back door or system vulnerability to gain access to its target. DDoS leverages the insecurity of other online devices. It assumes control and directs these compromised machines to target the legitimate entry points of target services that the attacker seeks to incapacitate. This reliance of compromisable connected devices such as CCTV cameras, advertising boards and a plethora of other Internet of Things (IoT) devices could be seen as a limiting (for the attacker), but the COVID-19 inspired, rapid move to home working in combination with the rise of smart cities has inadvertently inflated the quantity of potential resources available for use by DDoS (Cvitic et al., 2021).

As employees hurried to work from home, organisational IT equipment moved from inside the quality assured and monitored organisational security boundary, to networks shared with low grade and cheap IoT devices. And worse, these networks were often connected through home grade routers which incorporate rudimentary cyber security, many of which were configured by inexperienced home owners.

The move to smart cities involves the use of an ever-increasing supply of internet connected real-time data devices (Hammi et al., 2018). Through increased understanding of infrastructure patterns, residents could be provided with improved living experiences. However, as society becomes more reliant on this new technology, it may itself become an attractive target, and these devices may also form the resources needed for future larger-scale DDoS attacks.

Given that the majority of organisations in Australia rely on internet connectivity to conduct their business, they inadvertently expose themselves to a DDoS type cyberattack. It is therefore important to understand how organisations and their employees consider the threat and its associated consequences.

This paper aims to examine discovered gaps in knowledge of DDoS and brings together new learning to create a fuller picture of DDoS threats, motivations and the potential of future collaboration. The first research question asks "How high do Australian organisations rate DDoS as a threat, when compared to other cyber security events?" In particular, this research seeks to discover how employees and organisations perceive the threat, their ownership of the issues and consequences, and how they believe a future state should look. With this knowledge uncovered, a second research question asks "Where should effort be focused to ensure Australian organisations are more prepared for a DDoS event?", and if the 'where' is understood, the logical progression would be 'by who?' The overarching aim for this study is to demystify organisations' perceptions of the risk and threat of DDoS within the cyber security context and to uncover ways to improve the use of existing and future technologies.

The remainder of this paper is structured as follows. Firstly, a brief review of the literature is presented to set a clear understanding of the current knowledge in this area. Then, following an explanation of the methodology used, including a discussion on the reasons certain choices were made, the results of the research analysis are presented. Finally, the results are discussed and a conclusion approached so that a path is identified for future studies.

Literature Review

Practitioner Review

Cyber incidents appear to be placing an increased threat on society. Whilst DDoS has its beginnings at Illinios University's Computer-Based Education Research Laboratory (CERL) in 1974 (Dennis, 2010; Radware, 2017), cyberattacks including DDoS have increased in all forms such as scale, frequency and cost. In 2016 DYN, an Internet Domain registrar who helps the name resolution for many large, well-known, global firms including Twitter, Reddit, GitHub, Amazon.com, Netflix and Spotify (Krebs, 2016), suffered what was at the time, the largest DDoS attack, now known to be caused by the Mirai botnet. The attack at 1.2Tbps (Novinson, 2018) involved tens of millions of IP addresses (York, 2016) and was made possible by low security, poorly configured IoT (Internet of Things) devices such as security cameras (Cloudflare, 2019; Woolf, 2016; York, 2016).

In contrast to previous botnets constructed from infected PC's, Miria malware seeks to infect IoT devices such as security cameras, digital video recorders and baby monitors which have low security due to users installing with the default passwords in place (Cloudflare, 2019). Once installed, the malware deletes itself from the disk, but remains active in memory until the unit is restarted. The Mirai botnet source code was made available through 'Hackforums' (an Internet-based hacking community) in September 2016 (Manuel, 2018) shortly before the attack on DYN.

Then, in 2018, larger attacks occurred. In February, GitHub was attacked with a 1.3Tbs DDoS and, two months later, Netscout reported a 1.7Tbs attack against an unnamed target.

It was not a one-sided conflict though as, early in 2019, several successful prosecutions occurred:

1. The US Department of Justice seized 15 Internet domains, which they claim had been used to perform DDoS attacks on government systems, universities, gaming platforms, financial organisations and ISPs across the world (Kupreev et al., DDoS attacks in Q1 2019, 2019a).
2. A US court jailed a 34-year-old Massachusetts hacker (Martin Gottesfield) (Cimpanu, 2019; Wolff, 2019) for 10 years, for

launching the DDoS attacks on two medical facilities including the Boston Children's Hospital as he protested the psychiatric detention of Justina Pelletier (Wolff, 2019).

3. British police arrested 32-year-old Daniel Kaye who built a Miria botnet from hacked Dahua security cameras and other devices that he rented from other hackers (Daws, 2019). Kaye had been hired to ruin the reputation of Lonestar by a senior official at competitor Cellcom (a Liberian telco) (Daws, 2019).
4. 250 cybercriminals were arrested in Britain and the Netherlands by Europol (the European Union's law enforcement agency), following the 2018 shutdown of Webstresser.org (Krebs, 2019).

Despite these convictions, the scale, frequency and notoriety of these types of events have continued to increase such as:

- April 2019—Ecuadorian facilities became the target and very large number of cyberattacks including DDoS (Dan, 2019). Ecuador sought assistance from Israel (Kupreev et al., 2019b).
- 2019 September—Wikipedia was attacked with a DDoS volume of over 1Tbps over the three-day duration (Kupreev et al., 2019c).
- 2020 February—AWS reported an attack on its Connectionless Lightweight Directory Access Protocol (CLDAP) at a volume of 2.3Tbps.

In mid to late 2021, three DDoS attacks brought further increases in scale. The first, Cloudflare, which is a content delivery service, announced details of an attack on their infrastructure at a rate of 17.2 million bogus requests per second (rps) (Yoachimik, 2021). To put this in perspective, Cloudflare's average legitimate load is in the order of 25 million rps, so this attack occupied near 70% of its average capacity. Shortly after, a Russian tech company, Yandex reported an attack which started at 5.7 million rps in early August but peaked at 22 million rps one month later (Marrow & Stolyarov, 2021). Cyber security author Brian Krebs was also a target, announcing an attack in September 2021 which was delivered by the same botnet responsible for the attacks on Cloudflare and Yandex. This new botnet, called Meris, was first seen in June 2021 and was facilitated by approximately 250,000 compromised MikroTik routers (Krebs, 2021).

The incredible scale of these attacks is worrying, but more so is the fact that they have started to break away from the virtual world. For example, in 2005, Iran's nuclear development was impacted as an attack (Stuxnet) targeted supervisory control and data acquisition (SCADA) systems leading to destruction of physical centrifuge devices (Fruhlinger, 2017). In September 2007, the Israeli Airforce acquired control of Syria's air defence systems just prior to their military bombers targeting and destroying a Syrian nuclear installation (Holmes, 2018). Then, in March 2019, a DDoS focused on an electricity regulation computer system causing difficulties for various districts of Los Angeles and Salt Lake City. As a consequence, California and Wyoming also experienced power supply problems (Fazzini & DiChristopher, 2019).

More recently, in September 2020, a group mistakenly targeted the Dusseldorf University hospital and the disruption led to the death of a person who needed immediate and acute medical care (Tidy, 2020).

Trends are moving from small extortion-driven groups towards politically-motivated occurrences and, in addition, larger groups that use increased complexity and sophistication are becoming more prominent (Mansfield-Devine, 2015; Nazario, 2008). For example, secondary outcomes such as the insertion of malware or the theft of financial/personal data during an attack, highlight that DDoS is starting to be used as a cover for other nefarious activities (Pitlik, 2019; Wueest, 2014). In its study period, research company Neustar reported that 36% of responders had found malware installed during the event and 43% of finance sector responders also found malware further supporting that, DDoS attacks could be used as a diversion, masking the true purpose of theft (Sooraj, 2012). However, whilst geopolitical-motivated activism (hacktivism) has used this theft distraction method, they also use DDoS to show support or opposition over an issue.

Overall, the practitioner literature indicates that the DDoS phenomenon is growing, not just in scale, but also in its reach as it expands outside of the digital realm and begins to seriously impact the daily lives of ordinary people. However, this view, whilst supported by many independent sources (Chigada & Madzinga, 2021; De Donno et al., 2018; Snehi & Bhandari, 2021), is largely conveyed by technology vendors and authors who sit outside of the organisations directly impacted by these reported attacks. As such, the literature is unable to provide any supporting evidence to answer the first research question

"How high do Australian organisations rate DDoS as a threat, when compared to other cyber security events?".

In addition, the second research question "Where should effort be focused to ensure Australian organisations are more prepared for a DDoS event?" becomes equally difficult to answer using practitioner literature as most information is written by technology experts and focuses on technology mitigation options as opposed to a holistic view that also considers people and process.

Academic Review

Overall, several motivators for DDoS use have been noted (Anstee et al., 2017; Bienkowski, 2016) including Vandalism, State/activism, Extortion and Distraction, and although gaming related motivations appear high, criminal motivations are on the rise (Arbor, 2018; Bienkowski, 2016; Mansfield-Devine, 2015, 2016).

Criminals are learning to exploit the vulnerabilities that exist through the human interpretation of technology applications. The human factor often facilitates a weak link in cyber security (Wiederhold, 2014). As technology becomes 'smarter', it is moved from simple automation of repetitive tasks to assisting where decision-making is required and this advancement of technology has led to infrastructure and systems often being operated by individuals with little computer expertise (Ghafir et al., 2018). These individuals perceive their own level of threat, but as their experience of cyber threats varies greatly, threat perceptions amongst operators can be wide ranging and therefore, the actions they take in response may be equally diverse. In addition, individuals that consider the protection of their online identity a low priority may carry over this perception to the workplace, exposing organisations to cyber threats (Huang et al., 2010). The way individuals react to the discovery of an attack can be influenced by their own internal needs (McClelland, 2010) and these influences can stem from the community and culture in which they developed (Nisbett et al., 2001). As such, despite the agnostic nature of technology, its application by individuals and groups may differ and this may affect how cyber defence operations are conducted. Similar technology could be in place, but ultimate vulnerability may be highly variable.

However, organisational durability is demonstrated by robustness. That is to say, even those who have sustained significant attacks often continue to operate and address their vulnerabilities. They learn from experience and protect against human error with process, and against ‘shadow IT’ with policy. Learning from experience can kick start reactive innovation which helps to advance and develop organisational improvements but, with a lack of public transparency and knowledge sharing, this appears to occur in isolation.

The continued development of attack vectors shows attacking groups have also advanced, sharing vulnerability information and methods with other groups (Biros et al., 2008). Each side shows similarities in scale as there are small firms protecting their business and countries protecting their sovereignty, just as there are individuals aiming to infiltrate systems and countries aiming to gain advantage over their adversaries, but cyber security events are not weight-matched fights.

Despite this, generally, the balance of power has always sat with the defensive team. Organisations recover and continue to operate, even when affected by business-crippling attacks. However, COVID-19, may have adjusted that power balance (Lallie et al., 2021; Pranggono & Arabo, 2020). Rather than move slowly and iterate new cyber security developments, organisations had to respond rapidly to a dispersed workforce (Ostiguy, 2021; Pranggono & Arabo, 2020). COVID-19 brought organisational staff’s equipment out from under the protective wing of IT systems administrators and placed the burden of remote connectivity on to home grade un-tested infrastructure (Lewis, 2020), which often resembled the very same untrained-configured shadow IT that policies and processes aimed to eradicate. In this rapid environmental change, organisations that were comfortable with a minority of remote workers suddenly found themselves with the task of migrating hundreds or thousands of employees to home-based offices with little time to prepare and less time to test their solutions (Lewis, 2020). This increase in remote staff and the associated increase of IoT devices creates an environment where the attack vectors and entry points for cyberattacks have expanded exponentially (Khan et al., 2020; Pranggono & Arabo, 2020).

Whilst academic sources tend to agree that the threat of cyberattacks is increasing, the majority of the information used to express this view has been collated from literature provided by practitioner sources. It is therefore difficult to state the level of threat as perceived by Australian organisations, as there is little data to support any accretion. Thus, a gap in knowledge was identified, and whilst an answer to the first research question is proposed, it remains non-validated.

Similarly, for our second research question regarding the focus of effort, academic sources show collaboration, knowledge sharing, and training of a diverse workforce is likely to improve capabilities, but direct information from organisations is lacking. Therefore, a second gap in knowledge has been uncovered and the research in this area has merit.

Methodology

This study investigates from three perspectives: existing literature; published organisational information; and personal perspectives of those who work in industries.

As information was scarce, causal research, which is used to investigate causal relationships between dependant variables, would not suit the study's needs (Oppewal, 2010). So exploratory research, which is often used to develop research objectives, combined with an element of descriptive research, which is useful when objects require descriptive investigation, was chosen as the preferable initial approach. However, the majority of the study was qualitative in nature, supported by descriptive analysis that quantified the gathered data when required to help develop meaningful interpretations.

Examination of exiting literature used sources from both academic and practitioner sources to form a more complete and balanced view. Literature from professional and technical sources helped inform what was currently known about DDoS and the scale of threat, as perceived by industry and the methods of mitigation. Academic literature was examined so that previous research knowledge could be understood and compared to current and historical industry knowledge. In both cases, literature was gathered from books (physical libraries and book shops) and electronic sources such as: digital searches made through UNE's online library and their affiliates; Google Scholar; and ResearchGate, which led to information sources including websites, interviews (video and transcribed), white papers and commercial cyber security reports.

These wide range of sources were combined to develop a baseline of knowledge from which to build new understanding of the perceptions of individuals in Australian Organisations related to the DDoS cyber threat. The information gathered led to the discovery of several gaps in existing knowledge and this helped develop the research questions set the basis for deeper research.

As the literature review neared completion, 30 employees from small and medium Australian organisations were interviewed to gain their perspectives on the DDoS subject. In addition, websites from 47 Australian organisations were analysed with a mix of interviewed organisational staff and those that were approached but declined to participate. These participants and websites were sourced from a wide range of industry sectors including education, mining, construction and information media & technology. This method was used so that the results would have a mix of those organisations with employees who were willing to share insights and those who were not, with the potential that this may expose, differences between the two groups.

Data gathered during the website analysis was recorded in Microsoft Excel. This facilitated high level observations and simplified calculations during readability examination. The low quantity of academic and practitioner information fuelled the need for more targeted research into organisational perspectives of DDoS. The research began with broad observations of cyber security subject matter before drilling down to more specific DDoS-related information. However, due to the lack of DDoS-specific and Cyber Security information in general, primary data collection via interviews became a necessity.

Interviews were conducted via a mix of videoconference and face-to-face meetings, with audio recorded for later transcription. Once transcribed, transcriptions were imported into NVivo12. The move from face-to-face meetings to videoconference occurred as a result of COVID-19 restrictions that limited personal contact.

Excel and NVivo12 were then used to explore the data and produce analysis aligned with macro and micro themes. Macro themes were listed initially before being examined more deeply to uncover micro themes derived from the collected website information and the perceptions and opinions of the interviewed individuals. These new insights were considered along with the analysis of existing literature to bring new understanding of DDoS and the perceptions of Australian organisations.

Results and Discussion

The exploratory research began with the analysis of 48 industry websites, made up of organisations whose employees had been interviewed (19) and organisations that had not (29).

For the initial observation of whether the organisations shared security information on their website, the results showed that 48% of the websites analysed, publically shared some security information. Further examination showed that whilst the near half shared security information, most of those who did not also declined to be interviewed. This could be indicative of a fear of sharing sensitive information, a competition-driven reluctance to collaborate or priority-based decisions.

Participant response statistics may partially support a reluctance to share. Of the 110 participants approached, whilst only 2% formally declined, 61% did not respond and a further 10% who initially agreed ceased contact when interview arrangements were attempted (Fig. 1).

However, as shown in Fig. 2, whilst a greater number of male invitees were approached, proportionally more female respondents agreed to participate. This supports the Hofstead et al. (2010) view that feminine cultures show traits of nurturing, collaboration and protection.

The information that was shared covered a variety of categories. In some cases, organisations limited their information to policies and procedures that more applied to employees than customers. This occurred even when the organisations business permitted use of its technology and systems. In other cases, especially with vendor organisations, technology and product related information was made available. However, in many cases, and in contrast to 'privacy statements' and 'terms and conditions' information, cyber security information was not easily located. Often,

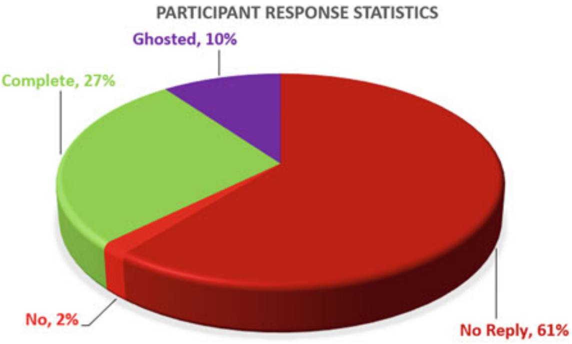

Fig. 1 Response statistics

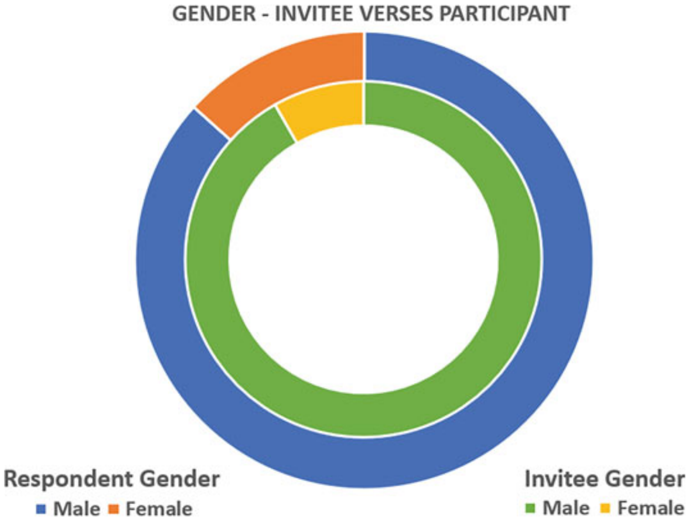

Fig. 2 Invitee versus respondent (Gender)

the information required a site search or the reader to follow a convoluted path to locate this type of information. Under Australian consumer law, all Australian websites are required to display terms and conditions for organisations that collect any customer or visitor information, privacy statements become a mandatory inclusion (OAIC, 2021). This is not the case for cyber security information as there are no current legal requirements to include this type of information. Any information shared is done so voluntarily and any organisation which does so is likely driven by organisational objectives.

Further website examination sought to uncover information related to strategic cyber security partnerships. This was included as notification of a partnership may indicate a preferred method of protection and an informal endorsement of a provider's capability. In the websites analysed, listed, partnerships were rare and only one website linked to the Australian Government's 'Scamwatch' program. Where as, others included links to vendors, who are often treated as partners and essentially did not operate in the security sector. Information about security partnerships were practically non-existent. Overall, very few mentioned any of their partners and, where they did, security partnerships were not included.

With little information publically presented, customers and consumers may be left to their own assumptions and understanding to invoke safe practices whilst using online resources. This initiates two considerations:

- Is the technology being used cyber secure by design?
- Is the technology being used configured for optimal cyber security?

As of October 2021, in Australia, minimum standards of cyber security for internet connected devices do not exist. Any network-compatible product purchased may or may not have cyber security features such as firewalls, encryption or access control lists. In fact, some devices, such as security cameras, may still operate with simple, well-known passwords (Shadman, 2017), despite this type of device's inclusion in the 2016 Mirai DDoS attack (Vlajic & Zhou, 2018).

In interviews, respondents raised the issue with product standards. Whilst Australian Consumer law directs minimum levels of safety and consumer satisfaction for all products available in Australia, it has no information directly related to the cyber security level of these products (The Australian Consumer Law, 2016). Products must be safe to use and function as advertised, but there is no legislation to ensure that they prevent unauthorised access or control. Similarly, whilst the ACCC has powers to govern compliance with legislation, it has no powers with respect to cyber security. Insecure products are still available in Australia and bad actors remain keen to exploit the vulnerabilities. It seems, only when consumers become aware of the risks, do they provoke change through purchasing preference (Blythe, 2020). Therefore, the pressure for manufacturers to develop safe and secure computer, network and IoT devices is driven by sector competition and consumer preference and, unfortunately, this comes at a cost (Blythe, 2020). As such, whilst the introduction of minimum levels of cyber security defence or standards for internet connected products and software could be one way to raise the level of protection for Australia's public and private infrastructure, it must be done jointly with methods of governance and auditing compliance.

Access to 'secure by design' technology is only one aspect of a secure implementation. Network connectable devices are often highly configurable and within the many options are choices that increase or decrease the level of security offered as a default by manufactures. As individuals may be influenced by their own threat perceptions, they have the ability to adjust the level of device protection so it is important that those configuring network devices have threat perceptions that are compatible with organisational decision-makers. In our interviews, most participants (20 of 30 interviewed) considered their perception of the threat of DDoS to be in line with their organisations. However, seven said that their organisation was less concerned than they were, with the remaining three stating their organisation was more concerned than themselves. This level of perception had an effect on cyber security budget approvals. Participants commented that justification for cyber security budget was more easily accepted if the organisation had experienced an attack, whereas those that possessed only theoretical knowledge were less keen to invest in prevention.

Information on attacks is scarce. Only one of the websites analysed listed details of a publicly-reported data breach, despite details of public data breaches being available for a further three organisations, from alternate public sources.

This lack of transparency could indicate a lack of trust between organisations and a lack of trust can prevent inter-organisational collaboration, as trust between people is an essential component of collaboration (Mitchell et al., 2011; Olson, 2019). Further, as cyber security relies on people as well as processes and technology (Herath & Rao, 2009), individuals carrying their own perception of online risk into the workplace (Huang et al., 2010) may support beliefs that the human factor remains the weakest link for cyber security (Kolenko, 2019; Wiederhold, 2014) and this can bring a significant effect on organisational vulnerability (Kolenko, 2019; Wiederhold, 2014). The human ability to assess threats relies heavily on human sensory detection (Blanchard et al., 2011), of which much is hidden when threats occur through digital methods. It is therefore necessary to provide training to improve human reasoning and behaviour. However, as psychological processes are susceptible to community and cultural influence, training and processes between groups may vary (Nisbett et al., 2001). It is therefore likely that outcomes can be different when technologies are implemented by differing groups and cultures and these differences may shift advantage to the defence. If cyber defence groups were able to collaborate more, they may be able to take advantage of differing perspectives and we may see more effective defence concepts being implemented even when using the same technology. This is a view supported by many respondents who, whilst claiming that more subject specific training was needed, also expressed a desire to see more real-world experience sharing between industries, countries, cultures, genders and ages, as a whole.

Conclusions

The field of cyber security is an interesting and fast paced place to be in the early 2020s. The explosion of IoT devices, greater than ever interconnectivity and organisational hunger for personal analytical data of life has further entangled continually innovated technology into our daily lives. Whilst this is partially driven by the need to efficiently reduce workloads and gain ever more understanding of our environments, it comes at a cost, as not all users of the data we generate, manipulate and share, have good intentions. Such is the rate of change, it can prove difficult to keep pace with daily new and evolving cyber threats that are continually discovered.

This study aimed to demystify some of the perceptions and assumptions of people and organisations and how they consider cyber threats against their personal and professional environments. This was a difficult task as little is written about the subject, but the exploratory research and qualitative analysis of the semi-structured interviews revealed some interesting new knowledge.

Firstly, despite the increase in network connected devices (including IoT), no product standards exist for cyber security products sold in Australia. This leaves consumers, including those with lower levels of computer literacy, holding the decision-making power without the protection of any consumer guarantees as to the products suitability for secure implementation. The introduction of an Australian standard would be one way to encourage manufacturers to design beyond a minimum requirement and, if policies are implemented intelligently, they could cover device configuration methods as, currently, consumers without adequate training face the task of configuring highly complex equipment in a way that protects their valuable digital resources.

The setup of standards may be one way to encourage greater collaboration. This study found little evidence of existing inter-organisational collaboration and very minimal transparency regarding each organisation's own cyber security defences. The difficulty in attracting participants further highlighted the reluctance of organisational staff to share knowledge that may help their peers. However, the study statistics showed that more female respondents agreed to participate than their male counterparts, which may further support the need for greater diversity in this area.

This study was undertaken during the COVID-19 pandemic and this had some effects on the cyber security landscape and the process of the study itself. During the pandemic, many staff needed to work from home and this placed a great load on organisation remote infrastructure. In many cases, urgency was focused on a rapid workable solution with security being a second consideration. For example, whilst company-owned laptops may have policy-driven security configurations, little to no audit would be performed on the home-based infrastructure to which it was connected. Therefore, COVID-19 rapidly changed the field of study and, with that, may have influenced the thoughts of the interview participants. This may also have had an effect on their willingness to participate but, at the very least, the interview process needed to adjust. Without the capability to perform face-to-face interviews, videoconferencing was used, altering the dynamic of the planned semi-structured conversations.

The implications of this study are broad. In one area, practitioners should aim for greater collaboration, as knowledge sharing and the opportunity to incorporate greater diversity of ideas and methods, may fuel development of more comprehensive implementations. In another, it is clear that, to date, greater academic focus has been placed on the technology and understanding how attacks are propagated and this has left the human side of cyber security under-researched. In a third area, more needs to be done regarding the way technology is designed along with attention to how adopters will configure the vast array of parameters available. Whilst manufacturers may begin to establish quality levels, policies may be required to ensure minimum standard are met.

This study was limited in scale due to the difficulty in obtaining enough participants to interview, but for future research, a deeper understanding of the motivation of people as they seek to protect their digital assets and further understanding of how they measure threat and risk when cyber security events cannot be seen or heard would be interesting to pursue and this may overlap into other areas of risk assessment where physical indicators are less obvious.

References

Akamai. (2016). *Akamai's [state of the internet]/security.* Retrieved from Akamai: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf

Akamai. (2020). *Akamai's [state of the internet]/security.* Retrieved from Akamai: https://www.akamai.com/content/dam/site/en/documents/state-of-the-internet/soti-security-a-year-in-review-report-2020.pdf

Alyas, M., Noor, M. I., & Hassan, H. (2017). DDOS attack detection strategies in cloud: A comparative study. *VFAST Transactions on Software Engineering, 5*(1), 36–43. https://www.vfast.org/journals/index.php/VTSE/article/view/502

Anstee, D., Chui, C. F., Bowen, P., & Sockrider, G. (2017, January 24). *Worldwide infrastructure security report.* Retrieved December 10, 2017, from Arbor Networks: https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf

Arbor. (2018, February 2). *Netscout Arbor's 13th annual worldwide infrastructure security report.* Retrieved from Arbor Networks: https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf

Bhattacharyya, D. K., & Kalita, J. K. (2016). *DDoS attacks: Evolution, detection, prevention, reaction and tolerance*. CRC Press.

Bienkowski, Y. (2016, August 2). *Denial of service & denial of access: Living in an era of cyber extortion.* Retrieved December 10, 2017, from Arbor Networks: https://www.arbornetworks.com/blog/insight/denial-service-denial-access-living-era-cyber-extortion/

Biros, D. P., Weiser, M., Burkman, J., & Nichols, J. (2008, January 12). *Information sharing: Hackers vs Law enforcement*. https://doi.org/10.4225/75/57a8260aaa0da

Blanchard, D. C., Griebel, G., Pobble, R., & Blanchard, R. J. (2011, March). Risk assessment as an evolved threat detection and analysis process. *Neuroscience & Biobehavioral Reviews, 35*(4), 991–998. https://doi.org/10.1016/j.neubiorev.2010.10.016

Blythe, J. J. (2020, January 8). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science, 9*(1), 1. https://doi.org/10.1186/s40163-019-0110-3

Chadd, A. (2018, July). DDoS attacks: Past, present and future. *Network Security, 7*, 13–15. https://doi.org/10.1016/S1353-4858(18)30069-2

Chigada, J., & Madzinga, R. (2021, January 1). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management, 23*(1), e1–e11. https://doi.org/10.4102/sajim.v23i1.1277

Cimpanu, C. (2019, January 10). *Anonymous hacker gets 10 years in prison for DDoS attacks on children's hospitals*. Retrieved from ZDNet: https://www.zdnet.com/article/anonymous-hacker-gets-10-years-in-prison-for-ddos-attacks-on-childrens-hospitals/

Claughton, D., & Beilharz, N. (2021, June 10). *JBS Foods pays $14.2 million ransom to end cyber attack on its global operations*. Retrieved from ABC News: https://www.abc.net.au/news/rural/2021-06-10/jbs-foods-pays-14million-ransom-cyber-attack/100204240

Cloudflare. (2019, October 2). *Famous DDoS attacks | The largest DDoS attacks of all time*. Retrieved from Cloudflare: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

Cook, S. (2021, May 16). *DDoS attack statistics and facts for 2018–2021.* Retrieved from Comparitech: https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

Crane, C. (2020, June 25). *Re-hash: The largest DDoS attacks in history*. Retrieved from The SSL Store: https://www.thesslstore.com/blog/largest-ddos-attack-in-history/

Cvitic, I., Perakovic, D., Perisa, M., & Botica, M. (2021). Novel approach for detection of IoT generated DDoS traffic. *Wireless Networks, 27*(3), 1573–1586. https://doi.org/10.1007/s11276-019-02043-1

Dan, A. (2019, April 16). *Ecuador claims it suffered 40 million cyber attacks since Julian Assange's arrest*. Retrieved from Tech The Lead: https://techthelead.com/ecuador-claims-it-suffered-40-million-cyber-attacks-since-julian-assanges-arrest/

Daws, R. (2019, January 14). *British hacker took down Liberia's whole telecoms network*. Retrieved from Telecoms Tech News: https://www.telecomstechnews.com/news/2019/jan/14/british-hacker-liberia-telecoms-network/

De Donno, M., Dragoni, N., Giaretta, A., & Spognardi, A. (2018). DDoS-capable IoT malwares: Comparative analysis and mirai investigation. *Security and communication networks*, 1–30. https://doi.org/10.1155/2018/7178164

Dennis, D. (2010, February 11). *Plato history*. Retrieved from Perhaps the first denial-of-service attack? http://www.platohistory.org/blog/2010/02/perhaps-the-first-denial-of-service-attack.html

Fazzini, K., & DiChristopher, T. (2019, May 2). *An alarmingly simple cyber-attack hit electrical systems serving LA and Salt Lake, but power never went down*. Retrieved from CNBC: https://www.cnbc.com/2019/05/02/ddos-attack-caused-interruptions-in-power-system-operations-doe.html

Fruhlinger, J. (2017, August 22). *What is Stuxnet, who created it and how does it work?* Retrieved from CSO Australia: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). March 26). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing, 74*, 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., & Khoukhi, L. (2018). IoT technologiesfor smart cities. *IET Networks, 7*(1), 1–13. https://doi.org/10.1049/iet-net.2017.0163

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

Hofstead, G., Hofstead, G. J., & Minkov, M. (2010). *Cultures and organizations: Software of the mind*. McGraw Hill.

Holmes, M. (2018). *Face-to-face diplomacy: Social neuroscience and international relations*. Cambridge.

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology, 29*(3), 221–232.

Ismail, S., Hassen, H. R., Just, M., & Zantout, H. (2021, October). A review of amplification-based distributed denial of service attacks and their mitigation. *Computers & Security, 109*, 102380. https://www.sciencedirect.com/science/article/pii/S0167404821002042

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). *Ten deadly cyber security threats amid COVID-19*. Retrieved from Taylors University: https://seap.taylors.edu.my/file/rems/publication/109566_7215_1.pdf

Kolenko, M. M. (2019). *Cyber defender cultural patterns and operational behavior.* Retrieved from ProQuest: http://search.proquest.com.ezproxy.une.edu.au/docview/2318150054

Krebs, B. (2016, October 21). *DDoS on dyn impacts Twitter, Spotify, Reddit*. Retrieved from Krebs on Security: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

Krebs, B. (2019, February 1). *250 Webstresser users to face legal action*. Retrieved from Krebs on Security: https://krebsonsecurity.com/2019/02/250-webstresser-users-to-face-legal-action/

Krebs, B. (2021, September 10). *KrebsOnSecurity hit by huge new IoT botnet "Meris"*. Retrieved from KrebsOnSecurity: https://krebsonsecurity.com/2021/09/krebsonsecurity-hit-by-huge-new-iot-botnet-meris/#comments

Kupreev, O., Badovskaya, E., & Gutn, A. (2019a, May 21). *DDoS attacks in Q1 2019*. Retrieved from Kaspersky: https://securelist.com/ddos-report-q1-2019/90792/

Kupreev, O., Badovskaya, E., & Gutn, A. (2019b, August 5). *DDoS attacks in Q2 2019*. Retrieved from Kaspersky: https://securelist.com/ddos-report-q2-2019/91934/

Kupreev, O., Badovskaya, E., & Gutn, A. (2019c, November 11). *DDoS attacks in Q3 2019*. Retrieved from Kaspersky: https://securelist.com/ddos-report-q3-2019/94958/

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021, June 28). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Lewis, J. (2020, April 9). *COVID-19 Insights—Emerging risks*. Retrieved from KPMG: https://home.kpmg/xx/en/home/insights/2020/04/covid-19-insights-emerging-risks.html

Mansfield-Devine, S. (2015, October). The growth and evolution of DDoS. *Network Security, 10*, 13–20.

Mansfield-Devine, S. (2016, November). DDoS goes mainstream: How headline-grabbing attacks could make this threat an organisation's biggest nightmare. *Network Security, 11*, 7–13.

Manuel, J. (2018, April 16). *Searching for the reuse of mirai code: Hide 'N Seek Bot*. Fortinet: https://www.fortinet.com/blog/threat-research/searching-for-the-reuse-of-mirai-code--hide--n-seek-bot.html

Marrow, A., & Stolyarov, G. (2021, Septeber 10). *Russia's Yandex says it repelled biggest DDoS attack in history*. (M. Potter, Ed.) Retrieved from Reuters: https://www.reuters.com/technology/russias-yandex-says-it-repelled-biggest-ddos-attack-history-2021-09-09/

McClelland, D. C. (2010). *The achieving society*. Martino Fine Books.

Mitchell, R. M., Ripley, J., Adams, C., & Raju, D. (2011). Trust an essential ingredient in collaborative decision making. *Journal of School Public Relations, 32*(2), 145–170. https://eric.ed.gov/?id=EJ935404

Nazario, J. (2008, July). DDoS attack evolution. *Network Security, 7*, 7–10. https://doi.org/10.1016/S1353-4858(08)70086-2

Newman, L. H. (2018, January 3). *GitHub survived the biggest DDoS attack ever recorded*. Retrieved from Wired: https://www.wired.com/story/github-ddos-memcached/

Nicholson, P. (2021, February 20). *Five most famous DDoS attacks and then some*. Retrieved from A10 Networks: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Nisbett, R. E., Peng, K., Choi, I., & Norenzayan, A. (2001). Culture and systems of thought: Holistic versus analytic cognition. *Psychological Review, 108*(2), 291–310.

Novinson, M. (2018, September 11). *8 biggest DDoS attacks today and what you can learn from them*. Retrieved from CRN: https://www.crn.com/slide-shows/security/8-biggest-ddos-attacks-today-and-what-you-can-learn-from-them

NSW Government. (2021, July 8). *The NSW department of education has been a victim of a cyber-security attack*. Retrieved from NSW Government: https://education.nsw.gov.au/news/media-releases/nsw-department-of-education-networks-

OAIC. (2021). *What is a privacy policy?* Retrieved from Office of the Australian Information Commissioner (OAIC): https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-a-privacy-policy/

Olson, D. (2019, April 22). *Trust—An essential collaborative component*. Retrieved from The University of Utah: https://law.utah.edu/trust-an-essential-collaborative-component/

Oppewal, H. (2010, December 15). *Wiley international encyclopedia of marketing: Causal research*. Wiley International. https://doi.org/10.1002/9781444316568.wiem02001

Ostiguy, P. (2021, February 16). *The distributed workforce is here to stay—Here's why performance matters*. Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2021/02/16/the-distributed-workforce-is-here-to-stayheres-why-performance-matters/?sh=4db2116e317c

Pitlik, D. (2019, July 1). *DDoS attacks growing ever-more sophisticated and efficient*. Retrieved from NetScout: https://www.netscout.com/blog/ddos-attacks-growing-ever-more-sophisticated-and-efficient

Pranggono, B., & Arabo, A. (2020, October 3). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters, 4*(2), 1–6. https://doi.org/10.1002/itl2.247

Radware. (2017, March 13). *History of DDoS attacks*. Retrieved from Radware: https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/

Shadman, R. (2017, February 2). *Default passwords for most IP network camera brands*. Retrieved from Custom Video Security: https://customvideosecurity.com/research/blog/default-passwords-for-most-ip-network-camera-brands/

Snehi, M., & Bhandari, A. (2021, May). Vulnerability retrospection of security solutions for software-defined cyber–physical system against DDoS and IoT-DDoS attacks. *Computer Science Review, 40*, 100371. https://doi.org/10.1016/j.cosrev.2021.100371

Sooraj, S. (2012, June 7). *Counting the cost of a DDoS attack: Computing, computing, June 7, 2012*. Retrieved December 20, 2017, from Gale: http://go.galegroup.com.ezproxy.une.edu.au/ps/i.do?&id=GALE|A292999416&v=2.1&u=dixson&it=r&p=ITOF&sw=w&authCount=

The Australian Consumer Law. (2016). *Consumers and the ACL*. Retrieved from Australian Consumer Law: https://consumer.gov.au/consumers-and-acl

Tidy, J. (2020, September 18). *Police launch homicide inquiry after German hospital hack*. Retrieved from BBC: https://www.bbc.com/news/technology-54204356

Turton, W., & Mehotra, K. (2021, June 5). *Hackers breached colonial pipeline using compromised password*. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Vlajic, N., & Zhou, D. (2018, July). IoT as a land of opportunity for DDoS hackers. *Computer, 51*(7), 26–34. https://doi.org/10.1109/MC.2018.3011046

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131–132.

Wolff, J. (2019, January 16). *Practice hacktivism at your own risk*. Retrieved from Slate: https://slate.com/technology/2019/01/martin-gottesfeld-hacktivism-ddos-boston-childrens-justina-pelletier.html

Woolf, N. (2016, October 27). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. Retrieved December 20, 2017, from The Guardian: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Wueest, C. (2014, October 21). *The continued rise of DDoS attacks*. Retrieved from Symantec: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/continued-rise-of-DDoS-attacks-14-en.pdf

Yoachimik, O. (2021, August 19). *Cloudflare thwarts 17.2M rps DDoS attack—The largest ever reported*. Retrieved from Cloudflare: https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/

York, K. (2016, October 22). *Read Dyn's statement on the 10/21/2016 DNS DDoS attack | Dyn Blog*. Retrieved from DYN: https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/