Cyber-Espionage: The New Era of Spying

BRYN DOWTON

Espionage has existed since the dawn of time, but since the introduction of the world-wide-web and connected devices (1970's), most spying is now done by data theft from computer networks [1]. Cyber-Espionage, or cyber-spying, is the act of obtaining information about individuals without their knowledge or consent through electronical means, it is a form of cyber-enabled crime (facilitated by ICT-connected devices, but not dependent on them). Within this essay I will delve into the features of the ever-changing technological era that have revolutionized this field. I will examine the spectrum of harm and the potential for mitigation, whilst also weighing the importance of national security against the rights to individua privacy. Furthermore, I will analyze multiple case studies to illustrate these points. The underlying thesis is that while cyber-espionage has transformed modern international security, it also poses unprecedented challenges to privacy, requiring a new outlook and reevaluation of legal and ethical frameworks.

Intelligence is built upon the collection of data and over the last 30 years we have seen a rapid development in data collection and, even more importantly, data storage which has only become possible due to the digital age. The first attempt of computationally storing data was the use of punch cards, with each hole representing an "on/off switch" to be fed into a machine, since then the methods of storing data have exponentially increased in efficiency with companies fighting for cheaper approaches for storing information [2]. In 2022, the amount of corporate data stored on the cloud surpassed 60%, making it the leading method of data storage amongst the leading companies in the world [3], and whilst this innovation essentially allows anyone access to unlimited storage, it raises serious concerns for safety. In parallel, the architecture of cloud computing opens the avenue for online anonymity, a critical area of espionage. Attribution is a term in the hacking community that relates to laying blame and the process of finding the real culprit, this has been clouded by the ability to operate under fake profiles, pseudonyms and many layers of digital protection (such as proxy IP addresses). A further feature of the digital age that has reshaped how spying is achieved is the vast accessibility, from a young age, anyone with intent and access to a computer can acquire knowledge in the field of cybersecurity, whether that be black hat (for malicious purpose), or white hat is due to the current moral and political setting of the individual, this will be explored in depth later on. Finally, the newly found role malware has within the scene of espionage cannot be overlooked, the use of hidden malicious code within ordinary-looking communication (emails and texts) has diversified the range of attacks that can be carried out. In the concept of cyber -espionage we are mainly talking about spear-phishing attacks, which are targeted attacks usually carried out on important individuals for leverage, monitoring and negotiation [4]. A notorious case of this was in 2011, when the RSA was hit with a severely personalized spear-phishing attack that ended up costing the company approximately $66 million, the attackers posed as an employee and hid the exploit code was within an attachment named "2011 Recruitment Plan.xls", a very normal seeming email with catastrophic effects for the firm [5].

Whilst cyber-espionage is mostly associated with governments, big corporations, militaries and infrastructure providers (systems providing power grids for example), any organization or individual which uses a computer is vulnerable against cyber operations [6]. The UK's secret service outlined primary areas of information that are targeted by international "spies"; Research (Academic findings, particularly in STEM), Business information and the Activity of Dissidents [7] are a handful of interesting area's that deviate the focus from previously political motives to a broader, more versatile understanding of cyber-espionage. Due to this new intent, worries about the potential increase of internal espionage and increased surveillance rise as the relationship between technology and society continues to be a complex area of discussion [8], especially while internal espionage continues to focus on certain demographics and political movements. A historical instance of the immoral application of internal espionage would be the Special Demonstration Squad (SDS), formed in 1968 in liaison with Mi5, the SDS was the policing body responsible for national security [9]. Throughout the 40 years that SDS operated, they were associated with the infiltration of over 1000 political movements, including pacifist organizations and anti-racist groups such as Youth Against Racism in Europe (YRE) [10], since the disbandment of the SDS, "The Undercover Police Inquiry" was established by Theresa May as a public inquiry to the actions of undercover police departments after revelations of the identities of dead children being used as officer names, the SDS had "particular prominence" in this ongoing investigation. This case study emphasizes that espionage is not restricted to governments and people of significant importance, with the everlasting argument of national security against personal privacy, the new digital appliance of espionage will allow a more versatile and mechanical approach to state surveillance.

The harm done by cyber-espionage has been shown to affect a wide range of people, however the strategic interests of governments and even countries will continue to be a barrier in regulating espionage with survival being an upmost priority [11]. As mentioned earlier, anybody with access to the internet has access to the knowledge needed to be a "cyber-spy" but the route in which they take in progressing this skill is still surrounded with confusion, one mitigation of harm would be more funding towards the teaching and discovery of youths who display the skills needed in the cyber-security field. Furthermore, a more ethical approach to the legislation and organizations created for national security is crucial for the safety of the individuals of a population.

In conclusion, the digital transformation of espionage and vast accessibility of the internet presents us with a paradoxical challenge: whilst cyber security measures need to be constantly updated for security (as seen with the RSA attack), these should not be taken advantage of for political gain. Democracies must balance national security with privacy, ensuring that surveillance measures put in place don't infringe with human rights. Addressing this challenge requires not only technological innovation but also ethical frameworks, reevaluation of laws and open communication regarding the surveillance being opposed on a population.

Bibliography

[1] - *Counterintelligence* (2016) *FBI*. Available at: https://www.fbi.gov/investigate/counterintelligence (Accessed: 16 March 2024).

[2] - Foote, K.D. (2017) *A Brief History of Data Storage*, *www.dataversity.net*. Available at: https://www.dataversity.net/brief-history-data-storage/ (Accessed: 16 March 2024).

[3]- *Percent of corporate data stored in the cloud 2022 | Statista*. (2023, September 28). Statista. https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/(Accessed: 16 March 2024).

[4]- Wangen, G. (2015). The Role of Malware in Reported Cyber Espionage: A Review of the impact and mechanism. *Information*, *6*(2), 183–211. https://doi.org/10.3390/info6020183

[5] - Sood, A., & Enbody, R. (2014). Infecting the target. In *Elsevier eBooks* (pp. 26). https://doi.org/10.1016/b978-0-12-800604-7.00003-6

[6]- Lindsay, J. R. (2021). Cyber espionage. In *Oxford University Press eBooks* (pp. 225). https://doi.org/10.1093/oxfordhb/9780198800682.013.12

[7] - *Counter State Threats | MI5 - The Security Service*. Available at: https://www.mi5.gov.uk/what-we-do/countering-state-threats (Accessed: 17 March 2024)

[8]- Turanjanin, V. (2022). When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights Approach. *International Cybersecurity Law Review*, *4*(1), p66. https://doi.org/10.1365/s43439-022-00074-7

[9] - Harper, D. J., Ellis, D., & Tucker, I. (2021). Covert aspects of surveillance and the ethical issues they raise. In *Advances in research ethics and integrity* (pp. 179). https://doi.org/10.1108/s2398-601820210000008013

[10] - Evans, R. (2020, April 16). Undercover police spied on more than 1,000 political groups in UK. *Police | the Guardian*. https://amp.theguardian.com/uk-news/2017/jul/27/undercover-police-spied-on-more-than-1000-political-groups-in-uk(Accessed: 17 March 2024).

[11] - Pun, D. (2017). 'Rethinking espionage in the modern era', Chicago Journal of International Law, 18(1), 369.