The Role of Big Tech in Future Cyber Defence

Angela Mison, Gareth Davies and Peter Eden
University of South Wales, Treforest, UK
Angela.Mison@southwales.ac.uk
Gareth.Davies@southwales.ac.uk
Peter.Eden@southwales.ac.uk

Abstract: Ordered society and nation states are dependent on interconnected systems, the defence of which is largely in private hands whose actions are driven by need for oligopolistic market dominance, protection of assets, and their monetisation models. This paper queries the responsibility of the nation state for the protection of itself and its citizenry. By some definitions, corporations are conducting cyberwarfare and, in cyberspace, are virtual nation states with ownership and rights over the data they hold and the intelligence it yields. The financial challenge for market dominance could drive an internecine war among the major technology corporations, and an assertion that the rights over the data they control are superior to those of the nation state. As functional monopolists, data they have acquired is not available from any other source. The intelligence from analytics exercised over that data, and the data itself is proprietary. These corporations exercise monopolist characteristics in the areas of data, information and intelligence. The aggregate value of the top 5 technology corporations, colloquially known as Big Tech is equivalent to third in projected global GDP rankings for 2021. This represents an equivalent expression of power in/over cyberspace. Cloud service providers (CSP) are often offshoots of Big Tech and have a high compound annual growth rate, thereby revealing the motivation for protection of market dominance and potential threat to user/customers. By concentrating on traditional cyber warfare and defence, there is limited consideration on policing or guarding against the rise of these virtual supranational powers driven by strict market agenda. What consideration there is regarding potential threats is driven by an economic perspective and anti-trust initiatives. Whether judged by the nation state as benign or malign, Big Tech has an impact on the nature and direction of society as currently understood and the question must be raised whether both citizens, organisations, and states need protection from it.

Keywords: Big Tech, Economic power, Surveillance capitalism, Information warfare, Cybersecurity

1. Introduction

1.1 The economic position of Big Tech

To the nation state seeking information, Big Tech are oligopolists for data, information and intelligence. Their motivations are strictly financial with respect to market dominance. Their extra-jurisdictional capacity enables them to put data beyond the reach of nation states in uncooperative jurisdictions, without the potential for retaliation, due to the dependence of nation states on the very organisations they may be seeking to regulate. Furthermore, their oligopsonistic position endangers and influences the direction of technological development, education, and exacerbates the skills shortage as their demand for specialist expertise increases.

Any form of market dominance can be detrimental to both customers and suppliers. Governments attempt to regulate the size and structure of market dominant organisations, requiring them to act independently of each other, and to promote competition for goods and services at beneficial prices (The Free Dictionary by Farlex, 2021). Historically, such anti-trust examples can be demonstrated by the break up of Ma-Bell in the United States of America and regulation of Microsoft in Europe.

1.2 Information warfare

There are many definitions of warfare in the digital sphere. Most mention the nation state and assume a political motivation, interfering with and potentially damaging information systems of the attacked entity. The suggested internecine war for economic market dominance could be seen in the light of the following definition where the battlefield is represented by the customer base and the combatants are big tech:

> *Information warfare is combat operations in a high-tech battlefield environment in which both sides use information technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information* (Wang & Li, 1995)

2. Is Big Tech an Oligopoly

There are technical economic definitions of market dominance for both the supply side and purchasing side. Oligopoly which relates to the supply side, describes a market in which there are a small number of players

present. Their products are closely related. It represents a competition among the few. This can be detrimental to customers/users as players can dictate both terms and prices. Where a customer is dependent on the good or service provided, the player can exercise undue or coercive influence over him.

Oligopsony is a purchasing market equivalent. Due to their purchasing power oligopsonists can dictate terms, prices, what is produced and where. Oligopsonists can have a collateral effect on other areas e.g. education for training to fulfil their needs or the direction and pace of research and development.

There is an argument that Big Tech does not represent an oligopoly, but that the constituent organisations operate in different markets. Where they compete, they are differentiated by behaviour and business models (Lotz, 2018).

It is suggested that Facebook and Google between them control 63% of the digital advertising market, and that advertising contributes to 97% and 88% of their revenues respectively. Both target consumers through algorithms. Their models of surveillance capitalism are well tried and profitable due to successful micromanipulation of users (Committee on the Judiciary, 2021).

Google achieves the bulk of its revenues from searches and has a pay per click business model, while Facebook uses gratis generation of attention-grabbing content and has a pay per view business model. Google makes a direct comparison of advertising revenue generated between its own search engine and Microsoft's Bing (Johnson, 2021), indicating a monitoring of potential challengers for market dominance.

There is a growing base of users of Google Cloud Platform and, using it as an example, it advertises 222% return on investment within 3 years and a payback on investment of 8 months. It is comprehensible that, in addition to other cost efficiencies (Lava & Marden, 2020), CSP are experiencing unprecedented growth.

Apple gains 84% of its revenues from hardware sales, where its profit margin is so high that market domination is unnecessary. It is a vertically integrated organisation, a silo, whose products are highly integrated and optimised when operating on its platforms. It is a growing platform conglomerate in that 11% of its revenues are generated through access to goods and services accessible through its platforms, e.g. media outlets and payment mechanisms (Vailshery, 2021).

Amazon is primarily a retailer, gaining 70% of its revenues directly from retail sales with 200 million unique visitor users per month (Hufford, 2020). For other retailers, Amazon acts as an intermediary. Businesses benefit through brand association. It is a platform conglomerate (AWS).

16% of AWS users are classified as large enterprise, while 84% represents Small and Medium sized enterprises, to whom outsourcing security and operational expertise, is part of addressing the skills shortage, cutting costs, and reducing their risk exposure. In the same manner as Google Cloud, Amazon sells the business value of AWS directly to the Board (Amazon Web Services, 2021). It does has sales documentation addressing cybersecurity (Rodgers, 2021), pertaining to the commissioning organisation, but not the security practices and procedures within AWS.

Microsoft predominates in the sale and licensing of software and, more recently, has entered the hardware market. Microsoft has an expansion strategy encompassing Cloud offerings, Azure. Azure is thought to have 4 Million customers globally (InfoClutch, 2021).

With the exception of Apple, a niche player, it is possible to agree that Big Tech is not necessarily an oligopoly, although they behave as such, and meet the criteria for oligopsony in their markets. While there have been concerns over the anti-competitive behaviour of Microsoft and Apple, they also demonstrate that there are advantages to oligopolistic supply and oligopsonistic diktat. The degree of interoperability available between disparate manufacturers is in part due to the running of the Microsoft operating system. The effective splitting of the mobile phone market between Android and Apple iOS epitomises the difficulty in achieving a balance between the pros and cons of any anti-trust action.

3. The absolute economic power of Big Tech

A country's comparative wealth ranking is usually made through use of Gross Domestic Product (GDP), the total value of all goods made, and services provided during a specific time period (HM Treasury, 2017). Corporate comparisons use market capitalisation. For the purposes of this section, the global GDP rankings, except for North Korea, are taken from (World Bank, 2021) while the market capitalisation for Big Tech are taken from (CompaniesMarketCap, 2021)

Currently, Big Tech comprises 5 USA based corporations. Taken individually, Big Tech corporations would rank between the fifth and sixteenth countries in the global GDP rankings. The aggregate market capital of the 5 organisations is $9.2 Trillion, roughly equivalent to the third largest global economy after the United States of America (GDP $20.9 Trillion) and China (GDP $14.7 Trillion). In comparison, the countries providing the greatest cybersecurity threat in addition to China are the Russian Federation (GDP $1.5 Trillion) and the Democratic Peoples' Republic of Korea (GDP $18 Billion), (Trading Economics, 2021). Chinese Big Tech, Tencent ($558 Billion), Alibaba ($407 Billion), and Baidu ($55 Billion) (Companies Market Cap (A), 2021) exhibit geographic market dominance.

Oligopsonistic power exercised over technology manufacturers, researchers, developers and education is revealed by consideration of the aggregate economic power of a purchaser with the world's third largest economy. Most recently the direction of the AI research may be subject to influence through funding provided to Universities by private corporations.

4. Big Tech and the growth of Cloud Services Providers

4.1 Market size, share, and trends

The economic power of Big Tech represents an equivalent expression of power in/over cyberspace. Big Tech has offshoot CSPs. A report on Cloud computing market size, share and trends (Grand View Research, 2021) provides the following details:

CSP are estimated to have a compound annual growth rate (CAGR) of 19.1%. With such a statistic, it is obvious that there is motivation for achievement and protection of market dominance. Big Tech has the resources for such competition. The global client spend on Cloud Services is estimated to be $1 Trillion, with a CAGR of 15.7%. The transition to the Cloud has accelerated due to the Covid-19 pandemic and the move to flexible and remote working.

For the individual consumer, the bulk of growth is seen in the Cloud Storage market where the major players are Apple, Alphabet (Google), Amazon, Microsoft, Box and Dropbox. The Cloud Gaming market is cross platform with an estimated 0.5 Billion users and a CAGR of 48%.

For businesses, the greatest area of usage for CSP is for business intelligence, supply chain management, enterprise resource planning and project and portfolio management. In terms of CSP revenue, X as a Service accounted for 60% of the revenue stream.

4.2 Cybersecurity and surveillance capitalism

What should not be forgotten in terms of cybersecurity is the balance of CSP revenue streams attributable to surveillance capitalism. Knowledge of an organisation, mode of operation and data gained through surveillance capitalism could be viewed as equivalent to an organisation's intellectual property, yielding the opportunity for such intelligence to influence negotiations with the CSP. Given the level of insider knowledge, this knowledge could be used by Big Tech to expand via merger and/or acquisition, increasing further their economic power. The business opportunity for OCG to expand their private Cloud operations to offer ‘legitimate’ Cloud services as a mechanism for money laundering through investment in legitimate businesses and opportunities for growth through use of such insider information is manifest.

Given the slick marketing of the business value of Cloud Services to the Board, it is easy to see that any cybersecurity technical queries raised with the Board may not carry sufficient weight to mitigate consequential outsourcing risks. The details of cybersecurity policies and protections applied internally to the CSP are, not without reason, a closed subject.

4.3 Oligopsony, oligopoly, and interoperability

The projected market dominance enables CSP to act as oligopsonists to their infrastructure suppliers, software suppliers, and academia, dictating both the direction and speed of technological development, advances in artificial intelligence and analytics, and the concomitant education required. The employment market also demonstrates this economic power. Organisations may have to accept the continuous provision of training positions as experienced personnel migrate to Big Tech with whom they cannot compete.

Competition and differentiation is already developing between the Big Tech constituents as they tussle for market dominance introducing a no return scenario for customers migrating to them. It is unlikely that any government or global organisational spend will be of sufficient quantity to influence the direction of Big Tech. Without interoperability, nations' dependence on CSP leaves them open to pressure and manipulation. For Big Tech, the fight for market dominance as CSP provides the battlefield for information warfare.

5. The costs of cyber defence and cybercrime

Robert Mueller III, a former FBI Director stated:

> *There are only two types of company: Those that have been hacked and those that will be hacked* (Mueller III, 2012)

There is an estimated global cybersecurity workforce shortage of 3.5 million (Moore, 2021) in a context where the global cost of cybercrime, $5.5 Trillion in 2020, is projected to rise to $10.5 trillion in 2025 (Nai, Fovino et al., 2020). Compared to GDP, the 2025 cost equates to the third largest global economy. Cybersecurity markets have a 2020 value of $200 Billion with a CAGR of 10% (*op cit*).

Revenues from cybercrime are of the order of $1.5 Trillion, 1% of global GDP, reputed to be greater than the profits of the global drug trade (McGuire, 2018), equivalent to the Russian Federation GDP (*ibid*). It has been suggested that some nation states benefit directly from cybercrime revenues and there are close links with money laundering (Office of Director of National Intelligence, 2021), (Miralglia, Ochoa et al 2012). With increased legalisation of drugs threatening to reduce organised crime group (OCG) profits, the logical business decision for OCG is to diversify into safer cybercrime with its low cost of entry and high return. To fully understand the volumes of money flowing through OCG, during the financial crisis of 2008, OCG is reputed to have supported the global economy (Spannaus, 2012).

Subcontracting by OCG could lead to an increase in Crime as a Service (CraaS) and introduce plausible deniability. McGuire [*ibid*] suggests that platform capitalism has been the intermediation model for CraaS. With revenues of $1.6 Billion, CraaS comprises sub and prime-contracted groups akin to a guerrilla army. The financial and human economics of guerrilla warfare are well known, as is the cost of defence against opportunistic cyber-attack. The situation portrayed in (Scott, 2004) has amplified with time.

In addition to the suggested business expansion schemes (Global Initiative Against Transnational Organised Crime, 2021), OCG have the means and patience to recruit, train, and retain the best, often behind legitimate business facades. A reported reinvestment programme of $300 million financed by revenues of cybercrime allows for investigation and development of new crimes, research on approaches not yet countermanded, and novel techniques (National Crime Agency, 2021). Defence against well-resourced, and motivated opponents is high cost. OCG cybercrime may represent a further example of information warfare involving market dominance.

6. The nation state, cybersecurity, information warfare, and anti-trust initiatives

Big Tech are using information technology, equipment and systems to attain their end - market dominance. Using the definition of information warfare [*ibid*], this maps directly to the rivalry over the power to obtain, control, and use information.

It is a State's responsibility to ensure an ordered society and the protection of its citizenry from all forms of warfare. Organisations, individuals, and even nation states are seemingly unaware of being victims in an internecine war, playing a very unequal part, and being on the losing side as they offer themselves and their information freely in exchange for business efficiencies and functionality.

Ordered society is dependent on the continuing and predictable behaviour of interconnected systems and the critical national infrastructure. The defence of such systems is largely in private hands whose levels of expertise, and knowledge of hyperconnected systems environment and complexity is unknown. In transitioning to the Cloud, elements of cybersecurity are being outsourced with no guaranteed access to policies, governance and procedures of providers and no inherent right to any data or the intelligence generated via analysis of that data.

The government can mandate what protections should be in place to ensure the continuity of operation of such systems, but a distinction can be drawn between compliance and performance. Technological advances mean that the knowledge for and complexity of securing any hyperconnected system cannot be determined, when a component is Cloud based. CSP are singularly reticent concerning their own cybersecurity, but Mueller's words [*ibid*] are apposite. If what organisations are protecting or securing cannot be defined, it increases the likelihood of cybersecurity failure. Such is the dependence on systems, that continuity plans are often sparse and/vague.

If governments, other organisations or individuals contract with CSP, legal entities in their own right, those CSP can relocate their corporate registrations and data repositories to the equivalent of cyber havens, rendering themselves extra-jurisdictional. In the worst case, uncooperative or seemingly over-regulatory governments could find themselves trapped in a technology without the portability and interoperability to enable them to transfer to another provider without interruption.

Anti-trust initiatives should be considered in this light. If Big Tech is broken up, the responsibility for continuity of operation of CSP must be specified. Contracts should include clauses concerning arrogation. The lack of available expertise for maintenance of the systems thus seized, is problematic, but seizure could extend a transition and migration period. Otherwise, undue pressure may be brought to bear on legislators or regulators for a less than optimum solution which exacerbates the potential for oligopolistic or oligopsonistic abuse.

7. Big Tech and data

Ownership of data is defined according to jurisdiction. Ownership of and rights to data is a particularly thorny issue that requires a paper in its own right (Scofield, 1998) (Northern Illinois University, 2021). There are two aspects of Big Tech and data that will be touched on here: the individual and the requirement for legitimate access to data by the nation state.

There is a United Nations initiative promoting data sovereignty, (Internet Governance Forum, 2020) which has been taken up by one of the internet founders (Berners-Lee, 2021). Such a move, giving individuals absolute right over their personal data and removing it from the control and ownership of Big Tech only partially addresses the problems caused by the growth of surveillance capitalism.

A possible extension to data sovereignty is the Swiss initiative examining the potential for the unification of online and offline presence to define an individual [*ibid*]. An online presence can be interpreted as an avatar, similarly to personality dissocoiative disorder. The individual becomes the sum his parts. The extension to unification of the person includes metadata. Metadata is part of the individual as it is data arising from actions and behaviours online. Such unification of the online and physical manifestations of the person, provides the state with investigative rights over its compound citizens.

Removal of such a major revenue stream arising from data would reduce the economic power and valuation of Big Tech and copious other industries. Extreme resistance can be expected. It could herald the advent of paid applications as organisations sought to recover losses. In the argument over privacy versus functionality, it is often stated there is '*no such thing as a free lunch*' (Heinlein, 1966).

While data sovereignty of the individual may ease the path of intelligence services and law enforcement agencies by giving them a quick route to some data access, what is sometimes of more interest and more informative are metadata and management data. Metadata arises from the system itself, thus there is an argument that with pure data sovereignity, there is no relation between the individual and data generated within the system.

Management data, useful inter alia for demand prediction and billing, is indubitably the property of the CSP, but may be extremely relevant with regard to an investigation. Access to strictly proprietary data may be difficult to argue, and its link to criminal investigations bears a resemblance to the proactive preventive activities of

Minority Report (Dick, 2017). Of note in this area, is the treatment of data requested to be retained and later demanded by the Congressional Committee investigating events of January 6 2021 and the legal arguments associated with it (Goltein 2021).

8. Big Tech, policy, law, intelligence and law enforcement

For interconnected systems there is a difference between physical location and system accessibility. With growing economic power and capacity to relocate, Big Tech can be considered supranational entities with jurisdictional issues arise over access to data (Mison, 2019). The entities involved in CSP operation and their location are often private to the CSP. There are some similarities between CSP and the banking industry. The nation state is hampered by jurisdiction and international law. Data is a highly mobile commodity.

There is no law governing cyberspace nor the creation of supranational entities. Policy makers should consider the possible fallout from information warfare and have requisite policies and statutes in place. Technological development, policy definition, and statute enactment move at radically different speeds. There is a need to anticipate cybersecurity needs. If the guess about the future is wrong, having the defence is not an issue other than cost, but not having it, could lead to chaos.

For nation states dependent for their continuing operation on Big Tech CSP, containing the power of Big Tech may be limited by that dependence. Due to inherent market dominant behaviour, and limitations of portability and interoperability, a major cybersecurity concern for the existing new and forthcoming digital transformation programmes is to avoid being locked into a platform or service. Without an acceptable means of exit, Big Tech can exert extreme pressure, forcing administrations to yield to their demands.

The importance of understanding outsourcing cybersecurity to the CSP leads to internal CSP cybersecurity failures and the consequential impact on clients and beyond. Notification is at the whim of the CSP and investigation is contained within it, with no rights for any independent authority which may exist. Where there is any dependence, there should be contractual obligations placed on the CSP that enable independent investigation and assessment by the nation state or its agencies. Such cybersecurity outsourcing exposes dependent systems to vulnerabilities on a scale not hitherto seen as evidenced by log4j CVE-2021-44228 (mitre.org, 2021).

9. Conclusion

Nation states concentrate on traditional cyber warfare and cyber defence in order to protect themselves and their citizenry from the machinations of others. Big Tech represents a different threat, a clear and present danger. Already there is increased complexity of interconnected systems, increasing cybersecurity and cyber defence costs. If Big Tech and CSP approximate to supranational powers, there will be a need to police and guard against the imposition of their market driven agendas. One of those vying for market dominance in the future may just be an OCG legitimate facade e.g. a VPN or CSP.

To assess the future impact on society of unconstrained and uncontrollable Big Tech, one need look no further than the American experiment and its results which have led to self-perpetuation and reinforcement of strong, radical division threatening democracy (Egan, 2020). Whether judged by the nation state as benign or malign, technology has a great impact on the nature of society as it is currently understood and the question must be raised whether they should be considered as an integral factor in the formation of any nation's or organisation's cyber defence plans.

References

Amazon Web Services, 2021. *Realizing Business Value with AWS.* [Online] Available at: https://aws.amazon.com/executive-insights/content/realizing-business-value-with-aws/ [Accessed 22 September 2021].

Berners-Lee, T., 2021. *Time Berners-Lee's plan to save the internet: give us back control of our data.* [Online] Available at: https://theconversation.com/tim-berners-lees-plan-to-save-the-internet-give-us-back-control-of-our-data-154130 [Accessed 22 September 2021].

Committeee on the Judiciary, 2021. *Algorithms and Amplification: How social media platforms ' Design choices shape our discourse and our minds* [Online] Available at: https://www.judiciary.senate.gov/meetings/algorithms-and-amplification-how-social-media-platforms-design-choices-shape-our-discourse-and-our-minds [Accessed 3 December 2021]

Companies Market Cap (A), 2021. *Largest Chinese companies by market capitalisation.* [Online] Available at: https://companiesmarketcap.com/china/largest-companies-in-china-by-market-cap/ [Accessed 27 September 2021].
CompaniesMarketCap, 2021. *Largest Tech Companies by Market Cap (B).* [Online] Available at: https://companiesmarketcap.com/tech/largest-tech-companies-by-market-cap/ [Accessed 27 September 2021].
Dick, P., 2017. *Minority Report: Volume Four of the Collected Stories.* London: Orion Publishing Group.
Doyle, C., 2002. *Market Definition and Dominance.* [Online] Available at: https://www.itu.int/osg/spu/ni/competition/Presentations/Market%20Definition%20-CDoyle.pdf [Accessed 22 September 2021].
Egan, PJ, 2020. *Elections 2020 – The Role of Social Media in US Elections* [Online]Available at: Elections 2020- The Role of Social Media in U.S. Elections - United States Department of State [Accessed 30 November 2021]
Global Initiative Against Transnational Organised Crime, 2021. *Organised Crime Index.* [Online] Available at: https://ocindex.net/ [Accessed 30 November 2021].
Goltein E, 2021. *Congress' access to individuals private communications: the Jan 6 Committee's troubling precedent* [Online] Congress' Access to Individuals' Private Communications: The Jan. 6 Committee's Troubling Precedent (justsecurity.org) [Accessed 30 November 2021]
Grand View Research, 2021. *Cloud computing market size, share & trends analysis report by Service, by enterprise size, by end use, by deployment and segment forecasts 2021 - 2028.* [Online] Available at: https://www.grandviewresearch.com/industry-analysis/cloud-computing-industry [Accessed 22 September 2021].
Hattangandi, V., 2017. *Market Dominance Strategies.* [Online] Available at: https://drvidyahattangadi.com/market-dominance-strategies/ [Accessed 22 September 2021].
Heinlein, R., 1966. *The Moon is a Harsh Mistress.* 1st ed. New York: Putnam.
HM Treasury, 2017. *Gross Domestic Product (GDP): What it means and why it matters.* [Online] Available at: https://www.gov.uk/government/news/gross-domestic-product-gdp-what-it-means-and-why-it-matters [Accessed 22 September 2021].
Hufford, J., 2020. *Amazon Statistics: Need to know numbers about Amazon.* [Online] Available at: https://www.nchannel.com/blog/amazon-statistics/ [Accessed 22 September 2021].
InfoClutch, 2021. *Installed base.* [Online] Available at: https://www.infoclutch.com/installed-base/cloud-computing-software/microsoft-azure/ [Accessed 22 September 2021].
Internet Governance Forum, 2020. *IGF 2020 #42 Personal Sovereignty: Digital Trust in the Algorithmic Age* [Online Discussion] Available at: https://www.intgovforum.org/en/content/igf-2020-of-42-personal-sovereignty-digital-trust-in-the-algorithmic-age-0 [Accessed 30 November 2020].
Johnson, J., 2021. *Google vs. Microsoft Advertising: US mobile click share 2021.* [Online] Available at: https://www.statista.com/statistics/223308/trend-in-impressions-on-google-and-bing-in-the-us/ [Accessed 22 September 2021].
Lava, S. & Marden, M., 2020. *The Business Value of Improved Performance and Efficiency with Google Cloud Platform.* [Online] Available at: https://services.google.com/fh/files/misc/idc_business_value_of_google_cloud_platform_whitepaper.pdf [Accessed 22 September 2021].
Lotz, A., 2018. *Big Tech isn't one big monopoly it's 5 companies all in different businesses.* [Online] Available at: https://theconversation.com/big-tech-isnt-one-big-monopoly-its-5-companies-all-in-different-businesses-92791 [Accessed 22 September 2021].
McGuire, M., 2018. *Nation States, Cyberconflict, and the Web of Profit.* [Online] Available at: https://images.marketingcontent.ext.hp.com/Web/HPMartech/%7Bbbbddbcf-1506-4a26-aaa2-db614096130e%7D_hp-bps-web-of-profit-report_APR_2021.pdf?elqTrackId=2756f4161eb1467e98921ad587b6e0b7&elqaid=436&elqat=2 [Accessed 22 September 2021].
Merriam-Webster, 2021. *Definition of Monopsony.* [Online] Available at: https://www.merriam-webster.com/dictionary/monopsony [Accessed 22 September 2021].
Miraglia, P; Ochoa, R; Briscoe, I; 2012 *Transnational Organised Crime and Fragile States* [Online] Available at: WP3 Transnational organised crime.pdf (oecd.org) [Accessed 30 November 2021]
Mison, A, 2019. *MSc Dissertation: Defining a method for successful use of evidence obtained from Cloud based data in prosecutions in England and Wales* University of South Wales
mitre.org. 2021. *CVE – CVE-2021-44228* [Online] Available at: CVE - CVE-2021-44228 (mitre.org) [Accessed 13 December 2021]
Moore, M., 2021. *Cybersecurity Employment Growth Report.* [Online] Available at: https://onlinedegrees.sandiego.edu/cybersecurity-jobs-report/ [Accessed 22 September 2021].
Mueller III, R., 2012. *Speeches: RSA CyberSecurity Conference, San Francisco, CA.* [Online] Available at: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies [Accessed 22 September 2021].
Nai Fovino, I; Barry, G; Chaudron, S; Coisel, I; Dewar, M; Junklewitz, H; Kambourakis, G; Kounelis, I; Mortara, B; Nordvik, J.p; Sanchez, I. (Eds.) Baldini, G; Barrero, J; Coisel, I; Draper, G; Duch-Brown, N; Eulaerts, O; Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina, V; Ruzzante, G; Sportiello, L;

Steri, G; Tirendi, S; 2020. *Cybersecurity, our digital anchor, EUR 30276 EN*, Publications Office of the European Union, Luxembourg,

National Crime Agency, 2021. *Money laundering and ilicit finance.* [Online] Available at: money-laundering-and-illicit-finance [Accessed 30 November 2021].

National Crime Agency, 2021. *National Strategic Assessment of Serious and Organised Crime.* [Online] Available at: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/533-national-strategic-assessment-of-serious-and-organised-crime-2021/file [Accessed 30 November 2021].

Northern Illinois University, 2021 *Responsible Conduct in Data Management – Data Ownership* [Online] Available at: Data Ownership (hhs.gov) [Accessed 30 November 2021].

Office of Director of National Intelligence, 2021. *Transnational organised crime - a threat to international security - manifests itself in various regions in different ways.* [Online] Available at: https://www.dni.gov/files/documents/NIC_toc_foldout.pdf [Accessed 30 November 2021].

Rodgers, C., 2021. *CISO Insight: Every AWS Service is a Security Service.* [Online] Available at: https://aws.amazon.com/blogs/enterprise-strategy/ciso-insight-every-aws-service-is-a-security-service/ [Accessed 22 September 2021].

Scofield, M; 1998. *Issues of Data Ownership* [Online]Available at: sPrint Version - Issues of Data Ownership | Business intelligence, data warehousing and analytics editorial from DMReview [Accessed 30 November 2021].

Scott, P. D., 2004. *Drugs, Oil, and war.* London: Rowman & Littlefield.

Spannaus, A., 2012. *Interview: Antonio Costa - Former UNODC Head talks about Drugs and the World Banking System.* [Online] Available at: https://larouchepub.com/other/2012/3917costa_drugs_banks.html [Accessed 30 November 2021].

Srnicek, N., 2017. *Platform Capitalism.* Polity Press : Cambridge.

Statista Research Department, 2021. *Facebook: number of monthly active users worldwide 2008-2021.* [Online] Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [Accessed 27 September 2021].

Statista, 2021. *Worldwide Amazon Users.* [Online] Available at: https://www.statista.com/statistics/829113/number-of-paying-amazon-prime-members/ [Accessed 22 September 2021].

The Economic Times, 2021. *Definition of Monopoly.* [Online] Available at: https://economictimes.indiatimes.com/definition/monopoly [Accessed 22 September 2021].

The Free Dictionary by Farlex, 2021. *Anti-trust Law.* [Online] Available at: https://legal-dictionary.thefreedictionary.com/antitrust+law [Accessed 22 September 2021].

Trading Economics, 2021. *North Korea GDP.* [Online] Available at: https://tradingeconomics.com/north-korea/gdp [Accessed 22 September 2021].

Vailshery, L., 2021. *Apple's revenune worldwide 2004-2021.* [Online] Available at: https://www.statista.com/statistics/265125/total-net-sales-of-apple-since-2004/ [Accessed 30 November 2021].

Wang, B. & Li, F., 1995. *Information Warfare.* [Online] Available at: https://irp.fas.org/world/china/docs/iw_wang.htm [Accessed 22 September 2021].

World Bank, 2021. *World Development Indicators.* [Online] Available at: https://databank.worldbank.org/data/download/GDP.pdf [Accessed 22 September 2021].

Zuboff, S., 2019. *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power.* 1st ed. London: Profile Books.