[dstl]

The Science Inside

Defence Science and Technology Laboratory

Futures Student Essay Competition

Top 10

November 2021

Ministry of Defence

Contents

Foreword by Linda Knutsen

I would like to congratulate all those who submitted an essay outlining their vision of future threats and opportunities. The high calibre of these thought-provoking entries gave us new perspectives and a unique insight into what may be important to the next generation of budding scientists. The ability to prepare for a variety of alternate futures is at the heart of everything we do and is vital in keeping our armed forces, and the public, safe. These essays showed a huge amount of interest and enthusiasm about science and technology and highlighted the importance of diversity of thought. It is heartening to imagine some of these young writers may one day be working alongside our world-class people creating the innovations of tomorrow.

Linda Knutsen

Division Head, Exploration

Introduction and winners

The Defence Science and Technology Laboratory (Dstl) launched a quest to uncover visions of the future from the brightest student minds in the UK.

Entrants answered the question: what do you believe to be the future threats or opportunities facing UK defence and security over the next 25 years?

The competition was open to undergraduate and postgraduate students based at UK academic institutions. This publication contains the top ten essays, alongside an honorary winner from Thornhill Community Academy.

Winner: Thomas Bradbury

Joint Second: Kirsty Goodman

Joint Second: Richard Brown

Third: Laurence Legon

Joint Fourth: Valerie Buckland

Joint Fourth: Neil Ashdown

Fifth: Edward Holland

Sixth: Fearghal Hughes

Seventh: Jack Suitor

Eighth: Nick Johnson

Honorary Winner: Khadijah Akuji

Essay Title: The Arctic Paradigm Shift: Value and Security from the United Kingdom's Perspective

Author: Thomas Bradbury

Institute: University of Exeter

Abstract

This paper analyses how the Arctic will undergo extensive change within the next 25 years through an enormous paradigm shift driven by climate change, and how this will elevate the region's strategic value to the United Kingdom. Analysing numerous academic sources, I determine that the Arctic will present valuable opportunities to the UK in terms of economic gain and soft power potential. However, this study also recognises the geo-political problems that could arise as the ice caps melt. Russia, as the regional hegemon, is likely to exert its authority and become a disruptive influence towards Britain and its allies. In addition, relevant multilateral institutions may come under strain as unprecedented security concerns emerge. Overall, I advocate for a balanced approach that supports British industry, science and innovation in the Arctic while exercising foresight on new conflicts that could pose a threat to British interests.

Introduction

The Arctic has long been misunderstood and neglected by British policymakers. As the highest and coldest region on the planet, the perception of the Arctic's strategic value has been diminished somewhat by the realities of harsh climate conditions and little economic feasibility. In addition, the United Kingdom has no realistic stake to claim for Arctic territory. As an Observer State for the Arctic Council, the UK is currently limited to soft-power foreign policy goals that aim to 'maintain the Arctic as a peaceful and stable region'[1]. Yet, climate trends will lead to a radically altered Arctic in the next 25 years as ice caps melt and trade routes emerge. With the UK's geographic and political proximity to the major stakeholders, the nation could benefit hugely from new economic opportunities that emerge. However, the Arctic is also likely to become an arena of conflict that poses tough security problems. Russia possesses a capabilities advantage over other states as the Arctic hegemon, and existing institutions currently lack the security enforcement that will be required in the future to foster stability. This study will highlight how the UK can maximise value and minimise security threats in the inevitable paradigm shift.

Climate Modelling

Predictions concerning the Arctic's future are derived from several academic studies that have analysed different climate outcomes. With numerous variables impacting how much ice melts in the Arctic in the coming decades, Melia, Haines & Hawkins used 'multiple climate-model simulations'[2] to determine the impact of both a 'low-emission scenario in line with the UN Paris climate deal' and a 'business as usual scenario where global greenhouse gas concentrations increase unabated'[3]. This study concludes that the models 'unanimously project that Arctic sea ice will continue in long-term decline beyond the middle of the century, regardless of the most

[1] HM Government, "Beyond the Ice: UK policy towards the Arctic", Polar Regions Department, Foreign & Commonwealth Office, 2018, p.7

[2] Dr Nathanael Melia, Professor Keith Haines & Dr Ed Hawkins, "Future of the Sea: Implications from Opening Arctic Sea Routes", Government Office for Science, July 2017, p.7

[3] *Ibid*, p.7

optimistic mitigation strategies'[4]. Akensov et al. cross-referenced several differing climate and geographic models to predict the future viability of ships utilising Arctic trade routes. Their study 'suggests that unescorted navigation in the high Arctic in summer may be as possible as the early 2030s-2040s and is probable after the 2050s'[5]. Hansen et al. utilised quantitative and statistical modelling to find that the Northern Sea Route could become economically viable 'as soon as 2040'[6] due to the current rate of ice melting. The timeframes posited by each study indicate that it is a matter of when, not if, the Arctic ice caps melt. Thus, there is a high probability that the Arctic becomes more accessible and strategically relevant within the next 25 years even in an optimistic scenario of limiting global greenhouse emissions. The UK needs to be prepared for this and adapt quickly to new Arctic trends that present significant opportunities and threats.

Business Potential

The United Kingdom is internationally recognised as a leader in finance and maritime industries which makes it well placed to procure additional business as firms become attracted to a more favourable Arctic climate. Maritime UK argues that the country has an 'unparalleled tradition of excellence in legal, arbitration, insurance, P&I, shipbroking and finance'[7]. In addition, 'London is home to the leading source of market information on the trading and settlement of physical and financial shipping derivatives in the Baltic Exchange'[8] – placing the UK as a market leader for regulation and seafaring reputation. In conjunction, the state heavily relies upon accessible sea routes for its own trade, with 'approximately 96 per cent of the volume of all UK import/export trade entering the UK through its ports'[9]. Currently, maritime business services 'contribute £4.4bn to the UK economy'[10] with the country also constituting a '35% share of global marine insurance premiums'[11]. Despite having no claim to the Arctic's natural resources, the country's expertise will become even more valuable as commercial shipping increases in the next 25 years.

This prospect is enhanced by studies that have found the Northern Sea trade route between Europe and East Asia to be '43% shorter than the routes around the Cape of Good Hope… and 25% shorter than routes via Suez Canal'[12]. With these cost savings to procure and pressure lifted on other bottleneck junctions, the increased value of Arctic routes will produce a symbiotic demand for financial services and risk. Currently, the NSR is said to be 'an unstable and vulnerable shipping environment'[13] due to an unpredictability of ice patterns, expensive problems with insurance and the shipping season typically lasting just 5 months. Yet, considering that most climate models indicate that these cost-raising factors will be reduced with future Arctic warming, it can be assumed that more firms will incorporate the Arctic into business

[4] *Ibid*, p.10
[5] Yevgeny Aksenov et al., "On the future navigability of Arctic sea routes: High-resolution projections of the Arctic Ocean and sea ice", *Marine Policy Journal*, Elsevier, 4th February 2016, p.312
[6] Carsten Ørts Hansen et al., "Arctic Shipping: Commercial Opportunities and Challenges", *Copenhagen Business School Maritime*, 2016, p. 55
[7] Maritime UK, "Maritime Business Services", accessed 9th May 2021, https://www.maritimeuk.org/about/our-sector/maritime-business-services/
[8] *Ibid*
[9] Melia, Haines & Hawkins, "Future of the Sea", p.19
[10] PwC, "The UK's Global Maritime Professional Services: Contribution and Trends", London: The City of London Corporation, April 2016, p.7
[11] *Ibid*, *p.7*
[12] Aksenov et al., "On the future navigability of Arctic sea routes", p.301
[13] Yiru Zhang, Qiang Meng & Liye Zhang, "Is the Northern Sea Route attractive to shipping companies? Some insights from recent ship traffic data", *Marine Policy Journal*, Elsevier, 6th August 2016, p.59

strategies. In fact, a joint study by the UK, Canada and Norway determined that there is already palpable interest from private firms to invest in the region, but they 'do not necessarily have the resources to do so'[14]. The UK is uniquely placed to provide these resources and must be opportunistic in doing so when the paradigm shifts.

Importance of Soft Influence

By respecting the 'sovereign justification of the eight Arctic states'[15] but still being impacted by future Arctic developments, the United Kingdom needs to build its soft influence to protect its interests in trade, security and science. At present, it has successfully choreographed an active and collaborative role in the Arctic that must be cultivated further. Predominantly, this strategy has been driven by the UK's world class research and innovation to help solve emerging Arctic problems – which should continue in the coming decades. With the region likely to radically change environmentally, there is huge potential for 'research, technology and innovation'[16] as new issues emerge. A recent £200m investment in building the RRS David Attenborough - a ship that can facilitate scientific studies in extremely harsh conditions - signals the country's ambition in securing 'the future of the UK as a world leader in polar research'[17]. Ideally, this translates into the UK holding influence as an Arctic leader in science and climate as the value of the region increases. It should be noted that currently just 3 Arctic states 'produce more Arctic science papers than the UK'[18], reflecting a presence matched only by the USA, Canada and Russia. In fact, the UK Science & Innovation Network, in 'promoting collaboration between Arctic States and British researchers'[19], has increased the 'number of Arctic-related projects from just one to five'[20] with Russia. This diplomatic channel could be a vital tool for stability as relations the West and Russia potentially deteriorate further.

The United Kingdom should also continue to actively participate in various Arctic multilateral institutions. For example, it sends representatives to numerous bodies like the Arctic Frontiers and Arctic Circle Assembly where key experts and stakeholders discuss findings and trends. Scotland and Northern Ireland also form part of the 'Northern Periphery and Arctic Programme'[21] that aims to exploit 'unique growth opportunities'[22] in the North and Arctic. Both regions are well placed to help meet increased volumes of transit, with Stornoway Port in Scotland recently envisaging that 'in 20 years ships travelling between Asia and Europe could be refuelling in Stornoway'[23]. Clearly, the paradigm shift in the Arctic can produce clear soft power benefits that the United Kingdom should maximise to protect its interests in the region.

Russia's Hegemony

The greatest future threat posed to British security in the Arctic undoubtedly stems from Russia, the dominant influence on the region. With the largest geographical landmass in the region, the Arctic constitutes a staggering '70-80% of its national territory'[24]. This presence has long encouraged Russian governments to maximise the importance of its Arctic strategy as other

[14] Wilton Park, "The Arctic in 2045: A Long-Term Vision", *Foreign & Commonwealth* Office, Jan 2016, p.7
[15] HM Government, "Beyond the Ice: UK policy towards the Arctic", p.7
[16] *Ibid*, p.8
[17] Melia, Haines & Hawkins, "Future of the Sea", p.18
[18] HM Government, "Beyond the Ice: UK policy towards the Arctic", p.10
[19] *Ibid*, p.12
[20] *Ibid*, *p*.12
[21] *Ibid*, p.9
[22] *Ibid*, p.9
[23] BBC Report, "Stornoway Port Authority in Arctic hub plan", 31st July 2013, [accessed 10th May 2021], https://www.bbc.co.uk/news/uk-scotland-highlands-islands-23515405
[24] Wilton Park, "The Arctic in 2045: A Long-Term Vision", p.6

states neglect the region, leading to an enormous capabilities advantage. In having the 'largest fleet of icebreakers in the world with 32 in total'[25] and recently 're-commissioning Arctic Cold War bases'[26], the Russian state will be able to monitor and disrupt trade passing through the Arctic - potentially disrupting British endeavours and influencing Arctic trade routes for geo-political gain. This hard power is also reflected with a build-up of military presence, training drills Russian transit fees for shipping that uses the Northern Sea Route. As such, Russia will likely further consolidate its dominant position as the Arctic draws more attention. In addition, Russia has a clear ambition to secure Arctic natural resources which could draw it into conflicts. With its economy dangerously dependent on the price of crude oil and other commodities, the inherent instability and trade deficit that 'exceeds $233 billion'[27] is a compelling motivation for Russia to secure more resources to 'offset the declining production from its ageing fields'[28]. A recent NATO report found that 'up to 95% of Russian gas reserves and 60% of Russian oil reserves'[29] could lie within Russia's Arctic zone – indicating that the state will use the Arctic to guarantee its economic and energy security in the coming decades.

In addition, the nature of Russia's leadership makes it a volatile adversary that could weaponise the Arctic as an additional way to challenge the UK and its Western allies in the future. As a Commons Committee report recently noted, the 'centralised decision-making allows the Russian government to carry out decisions at speed'[30] to great success in undermining the slower democratic processes of the West. In addition, the report notes that 'Russia considers the UK one of its top Western intelligence targets'[31]. As a prominent ally of NATO and several Arctic states, the United Kingdom is thus likely to face geopolitical challenges as Russia seeks to exert its hegemonic position in the region. Territory disputes with Canada and Norway have already surfaced but to little resolution. Also to note is that regional volatility could create serious problems for UK trade – a likely scenario when half of the eight Arctic Council states are 'top 20 trading partners for the UK'[32]. In addition, 'Norway supplies 30% of the UK's total energy'[33]. Therefore, the UK should seek to 'capitalise on its strengthened international relationships'[34] and ensure that a combination of alliances and deterrents ensure the future stability of the region. The reality is that there will be increased Arctic activity even under the most optimistic climate models, which inevitably 'provide potential for heightened tension'[35]. As such, the UK must display foresight in its dealings with Russia in the region.

Structural Weaknesses in Arctic Institutions

The Arctic paradigm shift also poses an existential problem to current Arctic institutions, many of which the UK participates in. The Arctic Council, as the most important institution, ultimately lacks the power to enforce sanctions and protect regional security. With a combination of

[25] Tim Marshall, "Prisoners of Geography", (London: Elliot and Thompson Limited, 2016), p.279
[26] Melia, Haines & Hawkins, "Future of the Sea", p.21
[27] Thomas Brodzicki, "Resource curse and the potential impact of COVID-19: the case of Russia", *IHS Markit*, 17th March 2020, accessed 10th May 2021, https://ihsmarkit.com/research-analysis/resource-curse-and-potential-impact-of-covid19-russia.html
[28] NATO Parliamentary Assembly, "NATO and Security in the Arctic", *Sub-Committee on Transatlantic* Relations, 7th October 2017, p.6
[29] *Ibid*, p.6
[30] Commons Report, "Russia", *Intelligence and Security Committee of Parliament*, printed 21st July 2020, p.29
[31] *Ibid*, p.1
[32] Melia, Haines & Hawkins, "Future of the Sea", p.18
[33] *Ibid*, p.18
[34] HM Government, "Government Response to the Intelligence and Security Committee of Parliament Report 'Russia'", CP 275, July 2020, p.7
[35] HM Government, "Beyond the Ice: UK policy towards the Arctic", p.21

permanent members and invitational observers, consensus on security was not reached when it was established in 1996. Instead, the flexible body acts as a 'knowledge-building institution for publishing results and recommendations'[36]. These recommendations can easily be ignored, and a recent NATO report noted that these structural weaknesses 'may prove to be insufficient to regulate interstate relations in the face of renewed international interest in the region'[37]. This concern also applies to other institutions like the Arctic Economic Council and the Arctic Circle Assembly, which both act more as forums for discussion than for any enforceable security policy. These weaknesses could elevate the role of NATO in the Arctic in the next 25 years, with five permanent members of the Arctic Council in membership. Indeed, a joint Report by the UK, Canada and Norway re-affirmed a belief in NATO's Article 5 to protect the region, guaranteeing support 'if a member state is faced with military threat'[38]. Therefore, the survival of NATO will be fundamental to future Arctic stability. With no other country having 'such a heavy presence in the region or is as well prepared to tackle the severity of the conditions'[39], Russia will be well positioned to target institutional vulnerabilities to maximise its Arctic gains as the paradigm shifts. In doing so, it could also defy current conventions such as UNCLOS. The UK must play a leading institutional role in stopping an over-exertion and offer resolute support to its Arctic neighbours, supporting NATO where applicable.

Conclusions

The Arctic will transcend current assumptions surrounding its strategic value to become an important area of influence for the United Kingdom in the next 25 years. The inevitability of climate change, re-affirmed by numerous models and quantitative studies, essentially guarantees that the Arctic's commercial and geo-political value will grow as the ice melts. The UK will stand to gain a lot through its financial and services expertise in the maritime industry and its proximity to Arctic routes. In addition, the UK can procure future soft power gains in the region as a world leader in Arctic science and innovation. However, the paradigm shift will grant Russia enormous influence as the clear hegemon in the Arctic. This could have dangerous consequences for British security with a potentially negative impact on trade and regional stability. The rapidly changing environment will also put strain on Arctic institutions, likely elevating the role of NATO as a security mediator in the region. Nonetheless, the UK is well placed to benefit from developments, but requires a balanced approach to maximise the opportunities and minimise security concerns.

Bibliography:

BBC Report, "Stornoway Port Authority in Arctic hub plan", 31st July 2013, [accessed 10th May 2021], https://www.bbc.co.uk/news/uk-scotland-highlands-islands-23515405

Brodzicki, T., "Resource curse and the potential impact of COVID-19: the case of Russia", *IHS Markit*, 17th March 2020, accessed 10th May 2021, https://ihsmarkit.com/research-analysis/resource-curse-and-potential-impact-of-covid19-russia.html

Commons Report, "Russia", *Intelligence and Security Committee of Parliament*, printed 21st July 2020

[36] Carsten Ørts Hansen et al., "Arctic Shipping: Commercial Opportunities and Challenges", p.76
[37] NATO Parliamentary Assembly, "NATO and Security in the Arctic", p.3
[38] Wilton Park, "The Arctic in 2045: A Long-Term Vision", p.6
[39] Tim Marshall, "Prisoners of Geography", p.268

Hansen, C. Ø., Grønsedt, P., Lindstrøm Graversen, C., & Hendriksen, C., “Arctic Shipping: Commercial Opportunities and Challenges”, Copenhagen: Copenhagen Business School Maritime, 2016

HM Government, “Beyond the Ice: UK policy towards the Arctic”, *Polar Regions Department*, Foreign & Commonwealth Office, 2018

HM Government, “Government Response to the Intelligence and Security Committee of Parliament Report ‘Russia’”, CP 275, July 2020

Maritime UK, “Maritime Business Services”, [accessed 9th May 2021] https://www.maritimeuk.org/about/our-sector/maritime-business-services/

Marshall, T., “Prisoners of Geography”, London: Elliot and Thompson Limited, 2016

Melia, N., Haines, K., Hawkins, E., “Future of the Sea: Implications from Opening Arctic Sea Routes”, *Government Office for Science*, July 2017

NATO Parliamentary Assembly, “NATO and Security in the Arctic”, *Sub-Committee on Transatlantic Relations*, 7th October 2017

PwC, “The UK’s Global Maritime Professional Services: Contribution and Trends”, London: The City of London Corporation, April 2016

Wilton Park “The Arctic in 2045: A Long-Term Vision”, *Foreign & Commonwealth Office*, WP1453, 20th – 22nd January 2016

Yevgeny Aksenov, Y., Popova, E., Yool, A., Nurser, A.J., Williams, T., Bertino, L., Bergh, J., “On the future navigability of Arctic sea routes: High resolution projections of the Arctic Ocean and sea ice”, *Marine Policy Journal*, 75, Elsevier, 4th February 2016, pp. 300-317

Zhang, Y., Meng, Q., & Zhang, L., “Is the Northern Sea Route attractive to shipping companies? Some insights from recent ship traffic data”, *Marine Policy Journal*, 73, Elsevier, 6th August

Essay Title: The Perils and Promise of Blockchain-Enabled Self-Sovereign Identity

Author: Kirsty Goodman

Institute: University College London

Abstract

The global pandemic has sped up the adoption of many emerging technologies. The convergence of some of these emerging technologies could radically alter fundamental societal processes. One example is the concept of 'self-sovereign identity' and parallel developments with blockchain technology. Self-sovereign identity is a proposed alternative to current identity administration. Its supporters call for individuals to have full control and ownership—or 'sovereignty'—of their own identity, versus the typically centralised, separate entity that traditionally controls a person's identity. The concept has gained recent momentum due to progress made within the blockchain ecosystem that enables the implementation of self-sovereign identity beyond aspiration, and the increasing adoption of the technology acts as an early indicator of the concept's feasibility. Proponents say that it offers more security, efficiency, and economic potential. However, peaks in crime have often followed technological innovations that lacked sufficient consideration of the repercussions, and history provides many cautionary tales of mass atrocities committed after nefarious use of identity related data. This essay seeks to provide an introduction to the concept of self-sovereign identity and an overview of likely perils and promise. It is hoped that with considerable forethought, the negative potential of self-sovereign identity can be mitigated, paving the way for policymakers to focus on realising the positive potential of self-sovereignty instead.

Introduction to Self-Sovereign Identity

Self-sovereign identity (SSI) is an ideological aspiration for a reformed identity management system (Giannopoulou and Wang 2020; Allen 2016). It strives to give the individual ownership and control over their own identity. This contrasts with current identity management where identity credentials are administered by a separate entity. Although the concept of identity is multi-faceted, traditionally an individual's ability to participate in society in various domains has depended upon formal administration of their identity (Ibid; Trulioo 2019). This takes place at multiple levels, from government institutions issuing formal proof of identification to social media companies controlling access to users' accounts. Currently, identity can be thought of as physically—and now digitally—fragmented, (Allen 2016; Milanovic 2017), and consequently wrought with security vulnerabilities. With identity ownership and control placed in the hands of a third-party institution, individuals are at risk of disenfranchisement and vulnerable to exploitation. Replacing current identity management models with one founded on principles of SSI is proclaimed to be more secure, (Andrade-Walz 2020) and could help expand societal participation to the estimated 1 billion today that lack formal identification (Desai, Diofasi, and Lu 2018).

The concept is gaining momentum with the parallel development of the blockchain ecosystem because the technology underpinning blockchain increases the feasibility of SSI. In 2019, Tobin explained how blockchain can enable the combination of three key SSI elements: i) "a secure connection" operating without a third-party provider ii) "digital data watermarking" for verifiability and iii) "a trusted, tamper-proof public key directory" (Tobin 2019). As the blockchain ecosystem

becomes institutionally embedded, there is hope that the ideological principles of SSI may come to fruition.

Perils

There is an assumption that blockchain-enabled SSI is tamper-proof because of its use of cryptographically secure decentralised identifiers. This high level of confidence in the technology could blind people to exploitable vulnerabilities in the future as the technology develops. There has been concern expressed over advances in quantum computing, for instance (Barmes and Bosch n.d.; Banafa 2019).

Additionally, digital technology requires a physical infrastructure (Walch 2019). This physical infrastructure remains vulnerable to socio-economic and geopolitical factors; for example, Denial of Service cyberattacks, state-sponsored takedowns, or energy output required for this transition. Additionally, a device can be protected with the most advanced cybersecurity available and still be breached by the human component of its defence (Fruhlinger 2019). Social engineering attacks will likely evolve, with criminals of the future finding new ways to exploit an individual's identity data for their own gain. Currently, there is the rising adoption of blockchain wallets for trading cryptocurrencies; however, ownership of this wallet is tied to a long seed phrase, and responsibility for protecting this seed phrase lies with the individual. It is an opportunity cost of removing the centralised intermediary institution that administers an individual's data. If an individual stores the seed phrase on their computer, however, and an offender finds access to that phrase, the offender would gain access and control over that person's wallet (Wang and De Filippi 2020). As blockchain technology use cases expand past crypto wallets and include more use cases centred on credential verification, more consideration would have to be given to the human dimension of keeping accounts secure. In its current form, this method of security is inaccessible to many and would leave those not as technically versed more vulnerable to social engineering exploitations.

From a societal perspective this could exacerbate systemic inequalities based on a digital divide. For example, this potential inaccessibility to the average user may spark a new security-as-a-service industry, such as providing account key protection; similar to the development of password managers as the complexity of passwords adapted in line with the average hacker's technical skills. However, it could widen the security gap between the rich and poor, whereby those with resources have access to more sophisticated protection. Outsourcing the security of seed phrases would also recreate a focal point of attack for cybercriminals—ironically replacing the intermediary that SSI aims to remove (Tobin 2019).

There are also implications from the new forms of identity commodification that blockchain-enabled SSI would allow. For example, blockchain technology has been heralded as an arbitrage between tangible and intangible assets with supporters claiming the technology would enable a marketplace for ideas and values (Taeed 2020). In combination with digitalised SSI, it could result in the extension of existing data commodification trends, potentially exacerbating current systemic inequalities. For example, in a system that enables the record keeping of previously intangible part identity, financial incentives for selling identity related data could result in a class system where the rich enjoy greater privacy and a continued 'right to be forgotten' (Wolford 2018), versus a poorer class subjected to greater surveillance and greater punishment for past indiscretions. Proponents say that decentralisation of the internet will correct the pitfalls of the web in its current form (Masnick 2019), which has contributed to polarisation and tribalism in online communities (Robb 2020). However, if the term 'cancel culture' were to take on a new

economic dimension[40], individuals could be pressured to conform to market driven norms, and divisions could widen—particularly as some groups in society may be penalised more than other groups for the same behaviours and/or opinions[41].

Additionally, although decentralised identifiers are cryptographically secure there is a risk of identity-related crimes and assaults posed by the transition of identity to its digital form should this data ever be compromised. This is particularly concerning when considering contemporary online community polarisation and reinforcing tribalism of the digital age, which could contribute to a digital "clash of civilizations" forecast at the end of the Cold War (Huntington 1993). Furthermore, the convergence of blockchain-enabled SSI with the rise of biometric technology for identity proof, could lead to a rise in biometric related assaults and identity theft involved with biometric data (Wang and De Filippi 2020). Finally, as personal identity becomes entwined within the digital domain, this may result in new forms of harassment and exploitation in personal relationships (Godin 2020). If a person's autonomy is compromised for example, then a shift to SSI may enable leverage of an individual's digital identity as a means of coercive control.

Promise

Nevertheless, with considerable forethought and strategic management of the risks presented, blockchain-enabled SSI shows promise. For example, as quantum computing advances, the security arms race has progressed with it, and new defenses against quantum attacks have been developed (Banafa 2019; Quantum Xchange 2018). Regarding individual security, proponents claim that blockchainenabled SSI would be more secure because it would shift to zero-knowledge proofs of identity (Andrade-Walz 2020). For example, any time you need to provide proof of age you must display identification that contains other sensitive identity credentials additional to your date of birth. This comes with a risk of identity theft. With zero-knowledge proof on the other hand, the technology interacts allowing the verification of the required information—for example, proof of age only—without the need for any data being read by humans (Civic 2018); reducing the risk of identity theft. The principle of minimisation in cybersecurity could serve as a further securitisation pressure driving the move to this technology in response to the recent cybercrime expansion (Jackson, Russell, and Sons 2017, chap. 4; BBC News 2021).

Blockchain-enabled SSI could also be economically beneficial. There is a significant cost of current identity management. As well as the time, labour and resources involved, society's potential to flourish can be hindered by what has been referred to as the economic cost of 'trust' (Kernel n.d.; Shea 2021). Blockchain technology on the other hand has trust built into the technology (Centre of International Governance Innovation 2018). Additionally, the bureaucracy of traditional forms of identity contributes to the exclusion of 1.7 billion people from accessing financial services (Lichtfous, Yadav, and Fratino 2018). Deloitte have estimated a $200 billion market opportunity from the financial inclusion of the "unbanked and underbanked". The UN World Food Programme, and UN Women's successful adoption of blockchain technology to improve aid delivery, has also shown the potential promise of blockchain-enabled SSI by demonstrating the technology's efficiency and cost reduction (Juskalian 2018; Thylin and Duarte 2019). Increasing State adoption is another indicator, for example Estonia, Finland, Thailand

[40] 1 Many social platforms being developed in the decentralised Web 3.0 infrastructure have a financial component, rewarding users for engagement; for example, BitClout has introduced an interesting dynamic through the combination of social media and tokenomics with users able to buy shares of themselves as well as other users they foresee being popular and thereby a lucrative 'investment' (BitClout n.d.).

[41] For example, Citron discusses the unequal punishment experienced by women compared to men when it comes to the weaponisation of deep fakes (2020).

and Singapore have already made headway with digital identity systems (Lim and Tay 2021). Furthermore, if blockchain technology successfully enables a marketplace of ideas and values through the arbitrage of tangible and intangible assets as proposed by Taeed (2020), there is potential for a vast untapped market when combined with SSI—perhaps akin to the economic growth that accompanied the invention of the company or loans.

In the long term, this could give rise to a geopolitical paradigm shift akin to the creation of the modern sovereign state with the Treaty of Westphalia in 1648. As the individual has autonomy over their identity and holds a diversified collection of credentials constituting their identity, geographic borders may no longer be as important in defining where an individual belongs. Estonia offers eresidency for example for digital entrepreneurs attracted to the EU (Republic of Estonia n.d.). With the incorporation of SSI, hypothetically an individual could opt into a community they would like to be associated with based on shared ideals and values versus traditional geographic boundaries.

Drawing upon Sampson et al.'s "typology of super controllers" in crime prevention (Sampson, Eck, and Dunham 2010), there are also proactive measures that may mitigate the negative impacts mentioned in the previous section, such as exerting regulatory pressure on the implementation of these identity systems to adhere to certain standards. For example, the UK Government's recently established Regulatory Horizons Council (Regulatory Horizons Council (RHC) 2020) in collaboration with civil society watch groups will be instrumental in informing the appropriate policy reform. To incentivise compliance, the government can introduce compensation to businesses that invest in new technical infrastructure while ensuring it meets minimum requirements. International organisations may have a role in ensuring open source and interoperable standards to maintain global collaborative security efforts. This could involve the creation of new global consortiums who issue guidance on best practices for SSI, such as the normative impact of the UN's Guiding Principles on Business and Human Rights(UN Office of the High Commissioner 2011). There are a few SSI alliances already attempting this (Decentralized Identity Foundation n.d.; ID2020 n.d.; Sovrin n.d.) that could act as super controllers and prevent crime by guiding SSI's implementation.

Regarding potential abuse of the technology, checks and balances will need to be established to prevent sanctioned misuse. The speed at which new forms of identity related crime emerge will require legislative reforms to be flexible while maintaining a punitive deterrent[42]. In a security conscious market however, the private sector may end up policing itself, for example via the market penalties incurred by companies that suffer security breaches, analogous to societal pressures driving corporate social responsibility initiatives today. If governments can implement measures that facilitate the above types of multi-stakeholder collaboration and holistic considerations, the transition to SSI may be a fruitful one.

Conclusion

After recent technological progress, self-sovereign identity (SSI) is on the horizon. Politically, states may be attracted to its bureaucratic efficiency and governance capabilities. Economically, it could create a vast untapped wealth and has the potential to counter the traditional cost of 'trust'. Socially, there is significant momentum due to its ideological appeal. Importantly, it shows convergence promise with other emerging technologies. This includes opportunities when combined within the blockchain ecosystem, and securitisation pressures, such as the necessity of the principle of minimisation in cybersecurity amidst a technologically driven cybercrime expansion. However, the potential of SSI is countered by the weight of its inhibitory pressures.

[42] From a rational choice perspective, effective legislation would likely alter an offender's cost-benefit calculations thereby discouraging them from committing the crime in question (Cornish and Clarke 2017).

Historical precedents of large-scale atrocities committed after identity related data was placed in the wrong hands are deeply concerning (Allen 2020). There would need to be checks and balances to prevent these kinds of atrocities from happening again. Additionally, it is reasonable to be cautious regarding the security concerns of such a nascent technology. Great care must be taken to avoid unintended consequences, such as the exacerbation of existing systemic inequalities and the creation of new ones. Nevertheless, with strategic forethought and a 'prevention through design' mindset (Ekblom 2017), governments may also reap rewards from self-sovereign identity.

References:

Allen, Christopher. 2016. 'The Path to Self-Sovereign Identity'. Life with Alacrity (blog). 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. ———. 2020. Ideology & Architecture of Self-Sovereign Identity | Odyssey Connect 2020. https://www.youtube.com/watch?v=JzM_Brpk95E.

Andrade-Walz, Alex. 2020. 'Self-Sovereign Identity: The True Password Killer'. Security, 2020. https://www.securitymagazine.com/articles/93356-self-sovereign-identity-the-true-passwordkiller.

Banafa, Ahmed. 2019. 'Quantum Computing and Blockchain: Facts and Myths'. OpenMind (blog). 26 November 2019. https://www.bbvaopenmind.com/en/technology/digital-world/quantumcomputing-and-blockchain-facts-and-myths/.

Barmes, Itan, and Bram Bosch. n.d. 'Quantum computers and the Bitcoin Blockchain'. Deloitte Netherlands. Accessed 10 May 2021. https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-thebitcoin-blockchain.html.

BBC News. 2021. 'US Treasury: Yellen Warns of "explosion" of Cybercrime Risk'. BBC News, 11 February 2021, sec. Business. https://www.bbc.com/news/business-56021100. BitClout. n.d. 'The Crypto Social Network'. Accessed 10 May 2021. https://bitclout.com/.

Centre of International Governance Innovation. 2018. What Is BLOCKCHAIN? The Best Explanation of Blockchain Technology. Lucas Mostazo. https://www.youtube.com/watch?v=3xGLc-zz9cA.

Citron, Danielle. 2020. Warped Reality : TED Radio Hour : NPR. TED Radio Hour : NPR. https://www.npr.org/programs/ted-radio-hour/929191205/warped-reality.

Civic. 2018. 'Anonymous Age Verifying Beer Vending Machine with Anheuser-Busch'. Civic Technologies, Inc. 12 May 2018. https://www.civic.com/blog/first-ever-anonymous-age-verifying-beervending-machine-in-partnership-with-anheuser-busch-inbev/.

Cornish, Derek B., and Ronald V. Clarke. 2017. 'The Rational Choice Perspective'. In Environmental Criminology and Crime Analysis, edited by Richard Wortley and Michael Townsley, 2nd ed., 29– 61.

Decentralized Identity Foundation. n.d. 'DIF - Decentralized Identity Foundation'. Accessed 10 May 2021. https://identity.foundation/.

Desai, Vyjayanti T, Anna Diofasi, and Jing Lu. 2018. 'The Global Identification Challenge: Who Are the 1 Billion People without Proof of Identity?' Blog. World Bank. 2018. https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-peoplewithout-proof-identity.

Ekblom, Paul. 2017. ‘Designing Products against Crime’. In Environmental Criminology and Crime Analysis, edited by Richard Wortley and Michael Townsley, 2nd ed., 304–29.

Fruhlinger, Josh. 2019. ‘Social Engineering Explained: How Criminals Exploit Human Behavior’. CSO Online, 25 September 2019. https://www.csoonline.com/article/2124681/what-is-socialengineering.html.

Giannopoulou, Alexandra, and Fennie Wang. 2020. ‘Self-Sovereign Identity’. Internet Policy Review, November. https://policyreview.info/open-abstracts/self-sovereign-identity.

Godin, Melissa. 2020. ‘How Domestic Abusers Have Exploited Technology During the Pandemic’. Time, 31 December 2020. https://time.com/5922566/technology-domestic-abuse-coronaviruspandemic/.

Huntington, Samuel P. 1993. ‘The Clash of Civilizations?’ Foreign Affairs 72 (3): 22–49. https://doi.org/10.2307/20045621.

ID2020. n.d. ‘ID2020 | Alliance & Governance’. ID2020. Accessed 10 May 2021. http://id2020.org/alliance.

Jackson, Craig, Scott Russell, and Susan Sons. 2017. Security from First Principles. O’Reilly Media Inc. https://www.oreilly.com/library/view/security-from-first/9781491996911/.

Juskalian, Russ. 2018. ‘Inside the Jordan Refugee Camp That Runs on Blockchain’. MIT Technology Review. 12 April 2018. https://www.technologyreview.com/2018/04/12/143410/inside-thejordan-refugee-camp-that-runs-on-blockchain/. Kernel. n.d. ‘Trust’.

Kernel. Accessed 10 May 2021. https://kernel.community/module-0/trust/. Lichtfous, Marco, Vivek Yadav, and Valentina Fratino. 2018. ‘Can Blockchain Accelerate Financial Inclusion Globally?’ Deloitte: Inside Magazine, 19 November 2018.

Lim, and Shirley Tay. 2021. ‘Infographic: Inside the Self-Sovereign Identity Revolution’. GovInsider Asia (blog). January 2021. https://govinsider.asia/transformation/infographic-inside-the-selfsovereign-identity-revolution/.

Masnick, Mike. 2019. ‘Protocols, Not Platforms: A Technological Approach to Free Speech’. Knight First Amendment Institute Columbia University. 2019. https://knightcolumbia.org/content/protocolsnot-platforms-a-technological-approach-to-free-speech.

Milanovic, Nik. 2017. ‘The next Revolution Will Be Reclaiming Your Digital Identity’. TechCrunch (blog). October 2017. https://social.techcrunch.com/2017/10/17/the-next-revolution-will-bereclaiming-your-digital-identity/.

Quantum Xchange. 2018. ‘Quantum Computing Will Break the Blockchain and QKD Can Save It’. QuantumXC (blog). 2018. https://quantumxc.com/quantum-computing-will-break-theblockchain-and-qkd-can-save-it/.

Regulatory Horizons Council (RHC). 2020. ‘Regulatory Horizons Council (RHC)’. GOV.UK. 2020. https://www.gov.uk/government/groups/regulatory-horizons-council-rhc.

Republic of Estonia. n.d. ‘What Is E-Residency | How to Start an EU Company Online’. E-Residency. Accessed 10 May 2021. https://e-resident.gov.ee/.

Robb, John. 2020. #959: Networked Tribalism: Filter Bubbles + AI Algorithms + Political Polarization | Voices of VR Podcast. https://voicesofvr.com/959-networked-tribalism-filter-bubbles-aialgorithms-political-polarization/.

Sampson, Rana, John Eck, and Jessica Dunham. 2010. 'Super Controllers and Crime Prevention: A Routine Activity Explanation of Crime Prevention Success and Failure'. Security Journal 23 (February): 37–51. https://doi.org/10.1057/sj.2009.17.

Shea, Michael. 2021. 'Ep. 146 – Self-Sovereign Identity and IoT – Insights from the Sovrin Foundation'. Insureblocks (blog). 31 January 2021. https://insureblocks.com/ep-146-self-sovereign-identityand-iot-insights-from-the-sovrin-foundation/.

Sovrin. n.d. 'The Sovrin Alliance'. Sovrin. Accessed 10 May 2021. https://sovrin.org/the-sovrin-alliance/.

Taeed, Olinga. 2020. 'Blockchain for Social Impact and Sustainability'. 101 Blockchains, October 5.

Thylin, Theresia, and María Fernanda Novelo Duarte. 2019. 'Leveraging Blockchain Technology in Humanitarian Settings – Opportunities and Risks for Women and Girls'. Gender & Development 27 (2): 317–36. https://doi.org/10.1080/13552074.2019.1627778.

Tobin, Andrew. 2019. 'The Three Pillars of Self-Sovereign Identity'. Evernym. 2019. https://www.evernym.com/blog/the-three-pillars-of-self-sovereign-identity/.

Trulioo. 2019. '100,000 Years of Identity Verification: An Infographic History'. Https://Www.Trulioo.Com. 13 November 2019. https://www.trulioo.com/blog/infographic-thehistory-of-id-verification.

UN Office of the High Commissioner. 2011. 'Guiding Principles on Business and Human Rights'. 2011. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

Walch, Angela. 2019. 'Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems'. In Crypto Assets: Legal and Monetary Perspectives, edited by Chris Brummer. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3326244.

Wang, Fennie, and Primavera De Filippi. 2020. 'Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion'. Frontiers in Blockchain 2. https://doi.org/10.3389/fbloc.2019.00028.

Wolford, Ben. 2018. 'Everything You Need to Know about the "Right to Be Forgotten"'. GDPR.Eu. 2018. https://gdpr.eu/right-to-be-forgotten/.

Essay Title: The WIMDs of change: present and future security concerns associated with Wearable and Implantable Medical Devices

Author: Richard Brown

Institute: Northumbria University

Abstract

The popularity of Wearable and Implantable Medical Devices (WIMDs) has risen dramatically in recent years and this technology is expected to be integrated into expanding medical networks in the years ahead. Data collection via networks of WIMDs promises to revolutionise healthcare by providing timely and effective diagnosis and delivery of care. The combination of big data practices with this emerging technology may provide vital insights into disease patterns and help to generate innovative health solutions. Despite boasting an array of potential benefits, the increased prevalence of WIMDs poses a threat to patient safety and national security. WIMDs may be hacked by malicious actors to administer fatal individual attacks or to overwhelm and disrupt critical infrastructure. The present and future national security risks associated with the emergence of WIMDs are likely to be underestimated. This is due to the unique vulnerability of this technology combined with the recent tendency to focus on data privacy issues when considering the potential impact of cybersecurity breaches. Greater attention should be given to the direct threat to life that hacks to WIMDs could cause, as well as the possibility for coordinated attempts to disrupt large medical networks. Future research should investigate the psychological and behavioural effects of interfering with WIMDs in order to mitigate the future risks of mass panic and societal disruption.

Introduction

The use of Wearable and Implantable Medical Devices (WIMDs) has exploded over the past decade and is expected to play an integral role in the delivery of healthcare in the forthcoming years. The ability to harness vast amounts of data from these devices could help to generate health solutions for a variety of long-term conditions, as well as to optimise the delivery of care. I will discuss the risks and security concerns associated with the increasing prevalence of WIMDs by considering the threat, vulnerability and potential impact of future attacks on these devices. The UK National Risk Register acknowledges the ability of cyberattacks to cripple essential networks such as the NHS (Cabinet Office, 2020). However, I will argue that the national security risks associated with the emergence of WIMDs are likely to be underestimated. This is due to the unique vulnerability of WIMDs and the tendency to focus on data privacy issues when considering the potential impact of security breaches. I will argue that greater attention should be given to the potential for direct attacks on individual safety, as well as the possibility for coordinated attempts to overwhelm and disrupt medical networks. I will also highlight the importance of considering the psychological and behavioural effects of interfering with WIMDs, and why this may threaten national security.

Wearable and Implantable Medical Devices (WIMDs): emergence, prevalence and future benefits

Wearable and implantable medical devices (WIMDs) represent a growing range of technology used for monitoring health and assisting in diagnosis and treatment. The latest generations of commercially available health trackers and smartwatches can be used to generate an array of health analytics by monitoring heart rate, blood pressure, blood oxygen, glucose levels, and respiratory irregularities (Liao et al., 2019). Implantable devices can also serve an active

function in maintaining health by automatically administering treatment. For example, insulin pumps, pacemakers and implantable cardioverter-defibrillators (ICDs) have long been used to manage long-term health conditions. WIMDs serve an important function as nodes in an expanding medical network by connecting patients and healthcare services through the Internet of Things (Jiang and Shi, 2021). This provides continuous data acquisition and the possibility for real-time information processing to administer timely diagnosis and treatment (Liao et al., 2019).

The increasing ubiquity of technology in recent years has led to a significant rise in the prevalence of WIMDs (Stiglbauer et al., 2019). This is expected to continue as commercial giants such as Apple, Google, Nike and Garmin look to generate innovative WIMDs in response to growing market demand (Casselman et al., 2017). The rise of WIMDs has thus been dubbed the dawn of a medical revolution (Dunn et al., 2018). Large healthcare institutions are predicted to initiate large rollouts of WIMDs in coming years as part of preventative care strategies (Dinh-Le et al., 2019). The use of WIMDs is expected to transform healthcare in the decades to come by enabling remote, continuous and longitudinal monitoring to provide automated health event prediction, prevention and intervention (Dunn et al., 2018). The next generation of WIMDs offer an exciting range of potential features such as the ability to detect cancer-related biomarkers (Yang et al., 2018) and recognise symptoms of infectious diseases such as COVID-19 (Ates et al., 2021).

The benefits to public health of using WIMDs include helping to identify long-term patterns of disease that would ordinarily be blurred by the daily fluctuation of symptoms (Austin et al., 2020). By using big data public health practices, the information collected by WIMDs can be analysed to provide insights into numerous health conditions, as well as to optimise the delivery of individual care (Roski et al., 2014, Hulsen, 2020). The effective use of WIMDs may also help to increase the efficiency of diagnosis and treatment in order to reduce the surging costs of long-term health care in the UK. In England, approximately 20 million people are currently living with a long-term health condition (Roddis et al., 2016). Due to the steady increase in life expectancy in recent decades (Vaupel, 2010), it is projected that the number of people with four or more chronic health conditions in the UK is likely to double by 2035 (Kingston et al., 2018). The annual total expenditure on long-term care in the UK is estimated to be £48.3 billion (Office for National Statistics, 2020). Therefore, the enhanced efficiency of diagnosis and treatment through the increased use of WIMDs in healthcare has the potential to reduce government expenditure and improve the nation's health.

Security concerns associated with WIMDs

In cybersecurity, risk is often calculated by applying the formula 'Risk = Threat x Vulnerability x Impact' (Jacobsson et al., 2016, Casselman et al., 2017).

Threat

The threat to health data from cyberattack is widely discussed (Luna et al., 2016, Kruse et al., 2017). In the US, the black market value of stolen health credentials is believed to be more than 10 times the price of a stolen credit card number (Humer and Finkle, 2014). This is likely to incentivise hackers to develop new strategies to infiltrate health networks. Additionally, a new class of threat has surfaced in cybersecurity known as Advanced Persistent Threats (APTs)(Deal, 2021). APTs constitute an active and sophisticated threat to governments and large institutions and are believed to be orchestrated by complex hacker groups and rogue nations (Chen et al., 2014). For example, the extensive disruption to the NHS from the 2017 WannaCry ransomware attack showed how medical networks can be targeted and that high profile attacks can damage public confidence in the ability of institutions to protect personal data (Saxena et al., 2019, Ghafur et al., 2019).

Vulnerability

WIMDs are uniquely vulnerable to cyberattack due to certain limitations that arise when designing medical devices (Woods, 2016). WIMDs are often required to be extremely small, and the immediate proximity to human flesh limits manufacturing options in terms of battery supply, computing power, memory space, heating and cooling (Woods, 2016). Therefore, many WIMDs are built without considering cybersecurity (Burleson and Carrara, 2014). Furthermore, connecting WIMDs to remote networks that exchange data irrespective of time and place raises the potential for data leakage and increases the vulnerability to attack (Jiang and Shi, 2021). As more WIMDs are used, there will be a rise in wireless body area networks (WBANs), which establish networks of sensors located both in and around the body to communicate seamlessly with one another and to automatically exchange data with existing devices such as smartphones (Casselman et al., 2017). Remote and mobile WBANs composed of inherently vulnerable WIMDs present a palpable threat to data security, and as recently highlighted, “these devices were not designed to withstand terrorist attacks.” (Woods, 2016).

Impact

Discussions concerning cybersecurity in health have typically focussed on risks to electronic health records from digital theft and related breaches to data privacy (Ronquillo et al., 2018, Ghafur et al., 2019). However, the potential impact of compromised WIMDs in expansive future medical networks poses a direct threat to patient safety as well as to the ability of medical networks to function. Such breaches also pose indirect threats to patients through the potential for inaccurate or doctored health readings that could lead towards misdiagnosis or ineffective treatment. Informational breaches of this severity could erode public confidence in medical networks and induce a state of panic by raising concerns for public safety.

Individual attacks. Firstly, it has been well documented that a range of WIMDs have been compromised in recent years (Beavers and Pournouri, 2019). For example, it was demonstrated at the Black Hat security conference in Las Vegas that an insulin pump could be remotely hacked and controlled from 200 feet away (Casselman et al., 2017). By broadcasting a stronger signal than the intended monitoring device, it was shown that blood glucose readings could be manipulated and that a lethal dose of insulin could be remotely administered. The potential for similar attacks on pacemakers and ICDs has also been shown. A team of ethical hackers demonstrated how they could gain remote access to a series of pacemakers in order to deliver fatal shocks (Pauli, 2016, Beavers and Pournouri, 2019). Additionally, the recent rise in digital theft by using contactless point of sale terminals on public transport to surreptitiously charge a victim’s credit card, has been suggested as a possible means of targeting pacemakers (Horton, 2016, Beavers and Pournouri, 2019). It may be possible to attack a pacemaker or ICD from close range by simply swiping a programmed reader across a victim’s chest (Beavers and Pournouri, 2019). These methods could plausibly be used for assassination attempts on individuals known to have implanted medical devices. It was reported that former US vice-president Dick Cheney requested that his doctor disable the wireless function of his heart defibrillator due to his belief that the technological vulnerability of WIMDs posed a credible threat to his life (BBC News, 2013). As implantable devices become increasingly pervasive across society, influential individuals could be targeted via their WIMDs if efforts are not made to bolster the cybersecurity of medical networks.

Network disruption. Additionally, manipulating the monitoring and tracking capabilities of WIMDs could threaten long-term health and damage the stability of medical networks.

For example, devices that are controlled to overlook health warnings could detrimentally affect patient health by failing to encourage medical consultation and intervention. Alternatively, devices that are manipulated to falsely detect symptoms of ill health may lead patients to urgently seek out unnecessary medical attention thus placing a strain on medical networks. If coordinated attacks were orchestrated across multiple devices, a surge in requests for urgent assistance could overwhelm healthcare services. Furthermore, if a large number of WIMDs already connected to a medical network were compromised, multiple devices could be controlled to send synchronised alerts to inundate medical networks, causing them to shut down. For example, a large number of cyberattacks involve Distributed Denial of Service (DDOS), in which a targeted network is flooded with superfluous requests from multiple corrupted sources (Kaur Chahal et al., 2019, Deal, 2021). Such attacks, choreographed across an extensive web of WIMDs, could cause devastating disruption to critical infrastructure in the UK, such as the NHS.

***Attacks on critical infrastructure*.** Hackers may also exploit the vulnerability of WIMDs to strategically target individuals that serve a particular function in an organisational network. Such a strategy could be used in coordination with additional focussed cyberattacks in order to infiltrate or disrupt critical infrastructure. For example, attempts could be made to neutralise known threat intelligence analysts and management operation leads at the National Grid by infiltrating their WIMDs to provide health warnings that urge them to seek out immediate medical attention. If such efforts were coordinated with focussed attacks on the cybersecurity systems of the National Grid, the remaining personnel may be ill equipped to repel the threat. In the US, former Secretary of Defence Leon Panetta stated that cyberattacks on critical infrastructure could result in “a cyber Pearl Harbour, an attack that would cause physical destruction and the loss of life.”(Panetta, 2012). It has been suggested that such a catastrophic cyberattack could arise through coordinated efforts to infiltrate and manipulate WIMDs (Woods, 2016).

Panic and societal disruption. Finally, WIMDs are expected to proliferate across medical networks and become an integral part of healthcare delivery (Dinh-Le et al., 2019). Therefore, it is likely that breaches to highly sensitive health data and potential threats to patient safety would provoke mass fear and panic. Inducing widespread panic is considered a form of information-psychological warfare that occurs due to a lack of reliable information about frightening phenomena (Panchenko, 2020). Malicious actors intent on undermining national security could look to provide misinformation via WIMDs in order to bring about a state of panic. For example, as future WIMDs are designed to detect symptoms of infectious disease to prevent outbreaks of viruses such as COVID-19 (Ates et al., 2021), the coordinated manipulation of WIMDs could instil an unwarranted sense of panic by reporting that an infectious outbreak was underway. Such attacks would erode public confidence in the ability of medical networks to provide reliable information, as well as having the potential to cause mass panic and societal disruption.

Conclusions and Recommendations

WIMDs have the potential to produce vast amounts of data that could be used to generate innovative healthcare solutions and optimise the delivery of care (Deal, 2021). The emergence of WIMDs, combined with big data practices, could become a goldmine for public health researchers. However, greater effort is needed to rectify some of the inherent vulnerabilities of WIMDs. Discussions of the cybersecurity of health data must go beyond considering threats to data privacy in order to address the direct threat to life posed by breaches to WIMDs, as well as the potential for future disruption and panic. Multi-disciplinary approaches that combine the expertise of cybersecurity specialists with behavioural scientists may also help to anticipate how

the public is likely to respond to future breaches to WIMDs and integrated medical networks. Such combined efforts may be able to enact strategies that inform the public of relevant risks in order to mitigate the potential for disaster whilst still being able to reap the benefits promised by this emerging technology.

References

ATES, H. C., YETISEN, A. K., GÜDER, F. & DINCER, C. 2021. Wearable devices for the detection of COVID-19. Nature Electronics, 4, 13-14.

AUSTIN, L., SHARP, C. A., VAN DER VEER, S. N., MACHIN, M., HUMPHREYS, J., MELLOR, P., MCCARTHY, J., AINSWORTH, J., SANDERS, C. & DIXON, W. G. 2020. Providing 'the bigger picture': benefits and feasibility of integrating remote monitoring from smartphones into the electronic health record: findings from the Remote Monitoring of Rheumatoid Arthritis (REMORA) study. Rheumatology, 59, 367-378.

BBC NEWS. 2013. Dick Cheney: Heart implant attack was credible. BBC Online.

BEAVERS, J. & POURNOURI, S. 2019. Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. Blockchain and Clinical Trial. Springer.

BURLESON, W. & CARRARA, S. 2014. Security and Privacy for Implantable Medical Devices, Springer.

CABINET OFFICE 2020. National Risk Register 2020. UK Government.

CASSELMAN, J., ONOPA, N. & KHANSA, L. 2017. Wearable healthcare: Lessons from the past and a peek into the future. Telematics and Informatics, 34, 1011-1023.

CHEN, P., DESMET, L. & HUYGENS, C. A study on advanced persistent threats. IFIP International Conference on Communications and Multimedia Security, 2014. Springer, 63-72.

DEAL, J. M. 2021. Exploring the Security Control Techniques Cybersecurity Specialists Need to Protect Medical Wearable Devices. Colorado Technical University.

DINH-LE, C., CHUANG, R., CHOKSHI, S. & MANN, D. 2019. Wearable health technology and electronic health record integration: scoping review and future directions. JMIR mHealth and uHealth, 7, e12861.

DUNN, J., RUNGE, R. & SNYDER, M. 2018. Wearables and the medical revolution. Personalized medicine, 15, 429-448.

GHAFUR, S., KRISTENSEN, S., HONEYFORD, K., MARTIN, G., DARZI, A. & AYLIN, P. 2019. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digital Medicine, 2, 98.

HORTON, H. 2016. Contactless card owners warned against public transport scanner hack. The Telegraph.

HULSEN, T. 2020. Sharing is caring—data sharing initiatives in healthcare. International journal of environmental research and public health, 17, 3046.

HUMER, C. & FINKLE, J. 2014. Your medical record is worth more to hackers than your credit card. Reuters. com US Edition, 24.

JACOBSSON, A., BOLDT, M. & CARLSSON, B. 2016. A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, 719-733.

JIANG, D. & SHI, G. 2021. Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare. Journal of Healthcare Engineering, 2021.

KAUR CHAHAL, J., BHANDARI, A. & BEHAL, S. 2019. Distributed denial of service attacks: A threat or challenge. New Review of Information Networking, 24, 31-103.

KINGSTON, A., ROBINSON, L., BOOTH, H., KNAPP, M., JAGGER, C. & PROJECT, F. T. M. 2018. Projections of multi-morbidity in the older population in England to 2035: estimates from the Population Ageing and Care Simulation (PACSim) model. Age and Ageing, 47, 374-380.

KRUSE, C. S., FREDERICK, B., JACOBSON, T. & MONTICONE, D. K. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25, 1-10.

LIAO, Y., THOMPSON, C., PETERSON, S., MANDROLA, J. & BEG, M. S. 2019. The future of wearable technologies and remote monitoring in health care. American Society of Clinical Oncology Educational Book, 39, 115-121.

LUNA, R., RHINE, E., MYHRA, M., SULLIVAN, R. & KRUSE, C. S. 2016. Cyber threats to health information systems: A systematic review. Technology and Health Care, 24, 1-9.

OFFICE FOR NATIONAL STATISTICS 2020. Healthcare expenditure, UK Health Accounts: 2018. Healthcare expenditure statistics, produced to the international definitions of the System of Health Accounts 2011.

PANCHENKO, O. 2020. Panic as a factor of information security threat. Public Administration and Law Review, 4-9.

PANETTA, L. 2012. Remarks by secretary Panetta on cybersecurity to the business executives for national security. New York City, 11.

PAULI, D. 2016. Fatal flaws in ten pacemakers make for Denial-of-Life attacks. Viitattu, 14, 2017.

RODDIS, J. K., HOLLOWAY, I., BOND, C. & GALVIN, K. T. 2016. Living with a long-term condition: Understanding well-being for individuals with thrombophilia or asthma. International journal of qualitative studies on health and well-being, 11, 31530.

RONQUILLO, J. G., ERIK WINTERHOLLER, J., CWIKLA, K., SZYMANSKI, R. & LEVY, C. 2018. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. JAMIA open, 1, 15-19.

ROSKI, J., BO-LINN, G. W. & ANDREWS, T. A. 2014. Creating value in health care through big data: opportunities and policy implications. Health affairs, 33, 1115-1122.

SAXENA, N., BHADORIA, R. S., DICKERSON, S., BRANCH, S., DALLEY, L. & CHURCHILL, N. 2019. Security and privacy issues in UK healthcare. Security and Privacy of Electronic Healthcare Records: Concepts, paradigms and solutions, 283.

STIGLBAUER, B., WEBER, S. & BATINIC, B. 2019. Does your health really benefit from using a self-tracking device? Evidence from a longitudinal randomized control trial. Computers in Human Behavior, 94, 131-139.

VAUPEL, J. W. 2010. Biodemography of human ageing. Nature, 464, 536-542.

WOODS, M. 2016. Cardiac defibrillators need to have a bulletproof vest: the national security risk posed by the lack of cybersecurity in implantable medical devices. Nova L. Rev., 41, 419.
YANG, Y., YANG, X.,

YANG, Y. & YUAN, Q. 2018. Aptamer-functionalized carbon nanomaterials electrochemical sensors for detecting cancer relevant biomolecules. Carbon, 129, 380-395

Essay Title: On the threat of a pandemic enabled by technological advances

Author: Laurence Legon

Institute: University of Warwick

Abstract

The 21st century has been referred to as “The century of Biology” due to the transformative potential that advances in biology possess. These new developments are making it easier to modify an organism to better suit our needs, which has the potential to benefit society in a number of ways. However, as these technological advances become more accessible, we need to be alert to how the abuse of these technologies could pose a threat to the nation’s security. One such way in which these technologies could be abused is with the creation of a man-made pandemic, which could have devastating consequences. Thus, it is important to the security of the nation for us to be aware of how ongoing research has, and will continue to, contribute to this mounting threat. In addition, we should acknowledge that the frequency at which pandemics occur is likely to increase as technology progresses, and ensure that our preparations for future pandemics take the threat of man-made pandemics into consideration.

Disease as a weapon

Throughout history, our species has been afflicted by disease and death caused by pandemics. This is widely considered to be a bad thing- so international efforts have been made to minimise or eliminate the burden of communicable disease upon the global population[43]. States have no incentive to oppose this as pathogens do not respect national borders; the spread of COVID-19 has highlighted how pandemic-causing pathogens in one country can pose a threat to the wellbeing of the entire globe[44].

In the past, militaries have deliberately spread diseases like smallpox or the plague to try and disrupt or kill their enemies[45]. Fortunately, however, in modern times we do not routinely see such diseases being weaponised. Pathogen-based bioweapons are prohibited by the 1925 Geneva protocol[46] and the 1972 Biological Weapons Convention[47], which impose political costs upon those who seek to develop or use them. However, these treaties lack enforcement mechanisms, and so cannot solely explain why states do not deploy pandemic-causing pathogens.

One alternative explanation for the lack of weaponisation of these pathogens is that they represent a double-edged sword. Transmissible pathogens can easily spread from enemy territory to your own people, and are also unpredictable due to their ability to evolve. In contrast, cyber and nuclear weapons can also cause mass disruption and devastation more predictably and with less risk of friendly casualties. Thus, utilising a pandemic-causing pathogen is rarely going to be the optimal choice for a modern, advanced military, which helps protect the public from man-made pandemics.

[43] UN General Assembly, “Transforming Our World : The 2030 Agenda for Sustainable Development.”
[44] 2 Carvalho, Krammer, and Iwasaki, “The First 12 Months of COVID-19: A Timeline of Immunological Insights.”
[45] National Academies of Sciences Engineering and Medicine et al., Biodefense in the Age of Synthetic Biology.
[46] United Nations, “Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare.”
[47] Conference of the Committee on Disarmament, “The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction.”

However, there are other groups that might see pandemics as a useful tool. Pathogen-based weapons would let individuals cause disproportionate amounts of damage as just a single infection can develop into a devastating pandemic. This potential might be of interest to deranged individuals who seek to cause mass killings, to terrorist groups, many of which show no qualms about targeting civilians or harming their own supporters, or as deterrents for states without the capacity to develop nuclear weapons[48]. There are several barriers that would make it difficult for these groups to create a pandemic, but technological advances may serve to wear down these barriers and raise the risk of man-made pandemics.

Weaponisation of existing pathogens

One key barrier to the use of pandemic-causing bioweapons is that most natural pathogens are not suitable for this. To be useful, the pathogen would need to have not already spread widely, yet also be transmissible enough that it could spread widely if given the opportunity, and there are not many pathogens that meet these criteria.

Smallpox is a prominent example of a disease that does. Smallpox is a viral disease that caused substantial mortality before mass vaccination campaigns resulted in its elimination in the wild in 1977. However, these vaccination campaigns have ceased, and the immunity they created has waned, so the release of smallpox would probably create a pandemic. American and Russian authorities hold the only infectious samples of the virus[49], and to date, have not tried to release it. Outside of them, access to the virus is controlled to prevent pandemics; for example, WHO guidelines prohibit researchers from possessing more than 20% of the viral genome[50].

However, recent biological advances have increased the risk of smallpox weaponisation. The smallpox genome sequence is freely available online[51], and it is possible to chemically synthesise viral genomes[52], so the smallpox virus's genome could probably be assembled. Furthermore, in 2017, infectious viral particles were made from a chemically synthesised genome of the closely related horsepox virus[53], and it is probable that the same methodology could be used to create infectious smallpox viruses. Thus, technological advances have raised the risk of a man-made pandemic by making it easier to obtain infectious copies of the virus.

There are also some natural pathogens that can cause widespread outbreaks of disease, and one of these pathogens could be isolated, cultured, and released by a group seeking to create a pandemic. Indeed, in 1993 the terrorist group Aum Shinrikyo tried unsuccessfully to obtain the Ebola virus for this very purpose, before settling for using non-communicable bioweapons and chemical weapons in their attacks on civilians[54]. Their failure demonstrates that weaponising a natural pandemic poses technical challenges- but if technological advances lessen these challenges, the risk of people deliberately spreading pathogens will increase.

Modification of existing pathogens

---

[48] Centre for Strategic and International Studies, "The Biological Weapons Threat and Nonproliferation Options."
[49] Riedel, "Smallpox and Biological Warfare: A Disease Revisited."

[50] World Health Organization, "WHO Recommendations Concerning the Distribution, Handling and Synthesis of Variola Virus DNA."
[51] National Centre for Biotechnology Information, "Variola Virus, Complete Genome."
[52] Cello, Paul, and Wimmer, "Chemical Synthesis of Poliovirus CDNA: Generation of Infectious Virus in the Absence of Natural Template."
[53] Noyce, Lederman, and Evans, "Construction of an Infectious Horsepox Virus Vaccine from Chemically Synthesized DNA Fragments."
[54]Olson, "Aum Shinrikyo: Once and Future Threat?"

In principle, a pandemic could be created by modifying existing pathogens to make them more infectious or lethal. However, while this is not impossible, it would likely require substantial resources and many skilled biologists, and as such is likely beyond the capabilities of an individual or small organisation. However, improvements in fields like genome engineering[55] and directed evolution[56] are making it easier to modify biology to suit our requirements, and this progress is only likely to accelerate as research interest and funding for synthetic biology increases.

Many of the deadliest pandemics in human history have been caused by zoonoses-animal pathogens that gained the ability to infect humans[57]. Thus, the engineering of animal pathogens to infect humans has the potential to create pandemics. Such research has been conducted in academic settings- for example, H5N1 avian influenza has been modified to make it transmissible between ferrets[58]. This was controversial as humans and ferrets have similar upper respiratory tracts, and so the mutations identified might also make the virus more infectious to humans. However, this controversy did not permanently stop this type of research[59], and proteins from H7N9 avian influenza have since been engineered to bind to human receptors more effectively[60]. Currently, this type of engineering requires substantial technical expertise, which lowers the chance of a nefarious individual successfully using it to create a pandemic, but this process is likely to become easier as genome and protein engineering improve.

Alternatively, a bioweapon could be created by modifying an existing human pathogen to make it more dangerous. The risk of this was made clear in 2001, where the ectromelia mouse virus was modified to express the immune signalling molecule IL-4. This let the virus subvert immune responses and become far more lethal, even to mice that were immunised or genetically resistant to the virus[61]. However, this is only one way in which pathogens could be engineered- it might be possible to make pathogens that attack new types of tissue, are drug resistant, or even cause chronic infections that delay the onset of symptoms until a trigger is detected[62]. While engineering a pathogen like this would likely be more challenging than tweaking animal pathogens to increase their ability to infect humans, advances in genome engineering, pathology, and immunology would make this easier, so this is also a risk that will increase as our biological capabilities grow.

Advances in structural biology may also make it easier to engineer pathogens to possess new functions. Classically, predicting protein structure has been challenging and has required difficult techniques and expensive, specialised equipment. However, AlphaFold promises to revolutionise the field by using deep learning to accurately predict protein structures from DNA sequences[63]. Learning about protein structure should help us understand how a protein's structure controls its function, which would then help us create proteins with novel functions.

[55]Gaj, Gersbach, and Barbas 3rd, "ZFN, TALEN, and CRISPR/Cas-Based Methods for Genome Engineering."

[56] Yang et al., "Synthetic Biology for Evolutionary Engineering: From Perturbation of Genotype to Acquisition of Desired Phenotype."

[57] Piret and Boivin, "Pandemics Throughout History ."

[58] Herfst et al., "Airborne Transmission of Influenza A/H5N1 Virus between Ferrets."

[59] Lipsitch, "Why Do Exceptionally Dangerous Gain-of-Function Experiments in Influenza?"

[60] de Vries et al., "Three Mutations Switch H7N9 Influenza to Human-Type Receptor Specificity."

[61] J. et al., "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox."

[62] National Academies of Sciences Engineering and Medicine et al., Biodefense in the Age of Synthetic Biology.

[63] Jumper et al., "Highly Accurate Protein Structure Prediction with AlphaFold".

Such a technology would have incredible potential- it might let us design enzymes that synthesise novel classes of chemicals, craft powerful biosensors to detect toxins, or identify new pharmaceuticals that interact with protein functional domains. However, such a technology would also make it far easier to design novel proteins that make pathogens more dangerous, and so advances in these fields need to be carefully monitored for new hazards that they might create.

What should we do?

Powerful new technologies are often associated with new dangers. Fire kept our ancestors warm- and killed them in deadly infernos. Fossil fuels transformed the way we travel- and now threaten our world through climate change. Advances in biology are no exception, as plenty of biological research that has the potential to benefit society can also be used for harm.

However, letting our vision be clouded by fear and completely restricting any technology with the potential for harm is not the answer. As biology advances, it can help us address major challenges that we face- it can help make industrial processes more sustainable, help us discover and synthesise novel pharmaceuticals, and vastly reduce the land and energy required to make food[64], and the risk of engineered pandemics should not stop this progress.

Ironically, it may be that advances that make it easier to create pandemics are also key to defeating them. While advances in structural biology might lead to engineered pathogens, structural biology can also help us find antimicrobials to fight these pathogens. Advances in viral engineering might make it easier to create viral pandemics, but these same advances might also help us engineer bacteriophages to tackle bacterial pathogens. These advances might let us swiftly eliminate future pandemics, and so it would be a tragedy if research restrictions from our fear of engineered pandemics condemned us to continue to suffer from natural pandemics.

That said, completely unconstrained research is not the answer either. Current ethical approval processes try and weigh up the risks and benefits of research, but care must be taken to ensure that they strike the right balance. For example, the researchers who created infectious poxviruses from synthetic DNA justified their research by claiming it might help create novel smallpox vaccines[65]. However, there are other ways that new vaccines can be made, and these methods would not have increased the risk of a smallpox pandemic being created. Therefore, in this instance, current ethical approval processes appear to have been insufficient to prevent risky research with questionable benefits.

Considering the dangers of new technologies is not just important for research approval, as identifying risks also helps us develop strategies to mitigate them. Covid-19 has made our vulnerability to pandemics clear, and new initiatives like the UK's Pandemic Preparedness Partnership[66] have already been devised to ready the country for future pandemics. However, since pandemics are likely to become more frequent as technology progresses, our precautions should be more rigorous to reflect this. We should also consider that future pandemics may be specifically designed to elude our countermeasures, and so we should try and increase our chances of having at least one working treatment against future pandemics by ensuring we do not put all our therapeutic eggs into a single basket.

[64] Aurand et al., Engineering Biology: A Research Roadmap for the Next-Generation Bioeconomy.
[65] Noyce, Lederman, and Evans, "Construction of an Infectious Horsepox Virus Vaccine from Chemically Synthesized DNA Fragments."
[66] Cabinet Office, Department of Health and Social Care, and Foreign Commonwealth & Development Office, "New Global Partnership Launched to Fight Future Pandemics."

All in all, the threat of a man-made pandemic will increase as technology advances. We should not seek to completely prevent technological advance, as the opportunities that new technologies bring outweigh the risks. However, to ensure the ongoing safety and security of the nation, the UK should acknowledge that the risk of man-made pandemics is going to grow, seek international agreements that restrict dangerous research that offers limited benefits, and above all ensure that we are as prepared as possible for when the next pandemic inevitably hits- regardless of whether the origins of this pandemic are natural, or otherwise.

Bibliography

Aurand, Emily, Jay Keasling, Douglas Friedman, Howard Salis, Chang Liu, Pamela Peralta-Yahya, James Carothers, et al. Engineering Biology: A Research Roadmap for the Next-Generation Bioeconomy, 2019. https://doi.org/10.13140/RG.2.2.16838.91208.

Cabinet Office, Department of Health and Social Care, and Foreign Commonwealth & Development Office. "New Global Partnership Launched to Fight Future Pandemics," 2021. https://www.gov.uk/government/news/new-globalpartnership-launched-to-fight-future-pandemics.

Carvalho, Thiago, Florian Krammer, and Akiko Iwasaki. "The First 12 Months of COVID-19: A Timeline of Immunological Insights." Nature Reviews Immunology 21, no. 4 (2021): 245–56. https://doi.org/10.1038/s41577-021-00522-1.

Cello, Jeronimo, Aniko V Paul, and Eckard Wimmer. "Chemical Synthesis of Poliovirus CDNA: Generation of Infectious Virus in the Absence of Natural Template." Science 297, no. 5583 (August 9, 2002): 1016 LP – 1018. https://doi.org/10.1126/science.1072266.

Centre for Strategic and International Studies. "The Biological Weapons Threat and Nonproliferation Options." Washington, 2006.

Conference of the Committee on Disarmament. "The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction." Geneva, 1972.

Gaj, Thomas, Charles A Gersbach, and Carlos F Barbas 3rd. "ZFN, TALEN, and CRISPR/Cas-Based Methods for Genome Engineering." Trends in Biotechnology 31, no. 7 (July 2013): 397–405. https://doi.org/10.1016/j.tibtech.2013.04.004.

Herfst, Sander, Eefje J A Schrauwen, Martin Linster, Salin Chutinimitkul, Emmie de Wit, Vincent J Munster, Erin M Sorrell, et al. "Airborne Transmission of Influenza A/H5N1 Virus between Ferrets." Science (New York, N.Y.) 336, no. 6088 (June 22, 2012): 1534–41. https://doi.org/10.1126/science.1213362.

J., Jackson Ronald, Ramsay Alistair J., Christensen Carina D., Beaton Sandra, Hall Diana F., and Ramshaw Ian A. "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox." Journal of Virology 75, no. 3 (February 1, 2001): 1205–10. https://doi.org/10.1128/JVI.75.3.1205-1210.2001.

Jumper, John, Richard Evans, Alexander Pritzel, Tim Green, Michael Figurnov, Olaf Ronneberger, Kathryn Tunyasuvunakool, et al. "Highly Accurate Protein Structure Prediction with AlphaFold." Nature, 2021. https://doi.org/10.1038/s41586-021-03819-2.

Lipsitch, Marc. “Why Do Exceptionally Dangerous Gain-of-Function Experiments in Influenza?” Methods in Molecular Biology (Clifton, N.J.) 1836 (2018): 589–608. https://doi.org/10.1007/978-1-4939-8678-1_29.

National Academies of Sciences Engineering and Medicine, Division on Earth and Life Studies, Board on Life Sciences, Board on Chemical Sciences and Technology, and Committee on Strategies for Identifying and Addressing Potential Biodefense Vulnerabilities Posed by Synthetic Biology. Biodefense in the Age of Synthetic Biology. Washington (DC), 2018. https://doi.org/10.17226/24890.

National Centre for Biotechnology Information. “Variola Virus, Complete Genome,” 2020. https://www.ncbi.nlm.nih.gov/nuccore/NC_001611.1.

Noyce, Ryan S, Seth Lederman, and David H Evans. “Construction of an Infectious Horsepox Virus Vaccine from Chemically Synthesized DNA Fragments.” PLOS ONE 13, no. 1 (January 19, 2018): e0188453. https://doi.org/10.1371/journal.pone.0188453.

Olson, Kyle B. “Aum Shinrikyo: Once and Future Threat?” Emerging Infectious Disease Journal 5, no. 4 (1999): 413. https://doi.org/10.3201/eid0504.990409.

Piret, Jocelyne, and Guy Boivin. “Pandemics Throughout History .” Frontiers in Microbiology , 2021. https://www.frontiersin.org/article/10.3389/fmicb.2020.631736.

Riedel, Stefan. “Smallpox and Biological Warfare: A Disease Revisited.” Proceedings (Baylor University. Medical Center) 18, no. 1 (January 2005): 13–20. https://doi.org/10.1080/08998280.2005.11928026.

UN General Assembly. “Transforming Our World : The 2030 Agenda for Sustainable Development.” New York, 2015.

United Nations. “Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare.” Geneva: United Nations, 1925.

Vries, Robert P de, Wenjie Peng, Oliver C Grant, Andrew J Thompson, Xueyong Zhu, Kim M Bouwman, Alba T Torrents de la Pena, et al. “Three Mutations Switch H7N9 Influenza to Human-Type Receptor Specificity.” PLOS Pathogens 13, no. 6 (June 15, 2017): e1006390. https://doi.org/10.1371/journal.ppat.1006390.

World Health Organization. “WHO Recommendations Concerning the Distribution, Handling and Synthesis of Variola Virus DNA,” 2016.

Yang, Jina, Beomhee Kim, Gi Yeon Kim, Gyoo Yeol Jung, and Sang Woo Seo. “Synthetic Biology for Evolutionary Engineering: From Perturbation of Genotype to Acquisition of Desired Phenotype.” Biotechnology for Biofuels 12, no. 1 (2019): 113. https://doi.org/10.1186/s13068-019-1460-5

Essay Title: What do you believe to be the future threats or opportunities facing UK defence and security over the next 25 years?

Author: Valerie Buckland

Institute: Lancaster University

Abstract

Technological advancements allow state actors such as China and Russia and terrorist groups such as ISIS and Hezbollah to exploit them and directly threaten the UK. Emerging technologies integrated with Artificial Intelligence (AI) systems such as micro drones, exoskeletons, advanced missiles, and cyber operations provokes AI arms race between major superpowers. Such technologies were once only a Sci-Fi vision but are rapidly becoming a reality. Russia and China being aggressors toward the UK will enable the utilisation of such technologies to further their strategic interests and undermine and destabilise the UK in order to secure their power and dominance internationally. As such technologies become cheaper and more easily accessible, terrorist groups are taking the opportunity to spread further hostilities at a greater distance, being almost undetectable. Ethical dilemmas around the use of such technologies by state actors and terrorist groups raise many concerns which are incompatible with a current ethical framework. It does not provide answers to the fundamental question of how a machine can be accountable for killings, creating a major ethical predicament. The use of such technologies for the purposes of strategic interests by state actors and magnifying terror by terrorist groups will act as severe threats facing the UK in the next 25 years. Building further resilience and effective deterrence will enable the UK to protect its nation, whilst enhancing its peace and security.

The Eye in the Sky
The eye in the sky is trying to hide
Lower the vision, less the collision
Two men in prison
Doubting freedom
Believing the motion
Of human emotion
One day they are free
Another they are gone
So that eye in the sky
Is not a friend, but a drone
-2020
Valerie Buckland

Introduction

When Kalashnikov invented the AK-47 he did not anticipate the global danger of his creation, let alone the drones, automated ballistic missiles, cyber bombs all integrated with AI. The true threat of such emerging technologies lies not only in the hands of autocratic leaders such as

Vladimir Putin or Xi Jinping but also terrorist groups such as ISIS or Hezbollah. The use of micro drones, exoskeletons, advanced missiles and cyberspace by state actors and terrorists are major threats which the UK will face over the next 25 years. Micro drone technology is advancing to the extent where spying, as well as lethally targeting an opponent, becomes almost undetectable. It allows new ways for state actors such as Russia and China to lethally target so-called enemies of the state within the UK's borders. Terror groups will also be able to exploit megacities to spread terror and undermine the UK's defence and security. The combination of exoskeletons and micro drones being developed by states such as Russia will become highly destructive. Advanced missiles integrated with AI will be developed by superpowers such as Russia and China, which calls for greater deterrence efforts to minimise such a threat to the UK. Terror groups will gain access to and utilise advanced missiles for their terror operations, making counter-terrorism efforts more challenging in the years to come. Operations within the cyber domain will be another major threat from Russia and China to destruct and interfere in UK's governments ventures but also, major public infrastructures. Information of Things (IoT) will enable terror groups to strengthen their operations in faster and more violent ways. This essay will discuss these threats in relation to ethical dilemmas, which will be a major challenge of the future.

Drones

Technological advances have transformed drones in military from enlarged and prominently visible to micro, almost invisible. Currently, 19 allied NATO states, including the UK, are in position of Black Hornet Nano. Russia and China are directly competing to overpower Western military capabilities, each aiming to become a leader in Artificial Intelligence (AI) technologies to lead the world (Pecotlc, 2019). Russia is preparing an army of micro drones(Young, 2020), which can freely and effectively spy, target and even poison the subject. Such operations would be invisible, and the trace difficult to detect, unlike the poisonings of former spies Sergei Skripal and Aleksandr Litvinenko by Russia on UK soil (BBC, 2018). This army of drone with the capacity to swarm could be stored in an AI powered advanced exoskeleton, similar to Ratnik-3 and Ratnik-4, but much more advanced (Konaev et.al, 2019). Likewise, China has recently created a micro drone Fengniao (Zhen, 2021) which could be used to steal intelligence from within the UK, unobserved and from a great distance. Clearly, the position and capabilities of such lethal technologies present a major threat to the UK's defence and security during the next 25 years.

Terrorist groups such as ISIS and Hezbollah have used drones to perpetrate attacks from a distance without committing suicide bombings. Commercial drones are becoming readily accessible and terror groups use them to commit evil and cause disruption. Terror groups are already experimenting with 3D printing micro drones, whilst exploiting their lethal capabilities (Pledger, 2021: 3) to cause hostilities, create public fear (Harari, 2019: 188) and directly threaten nations, whilst spreading terror on a greater level. Terrorist groups' potential use of micro drones with lethal intentions can be catastrophic in the scenario of dispersing 'deadly agents or viruses' (World Economic Forum, 2018) over large venues within urban environments. Terror groups could tactfully utilise micro drones in urban terrains (Bunker, 2015: 32) such as

London or Manchester, by blending in with the chaotic dynamics of the cities. Cities such as London and Manchester are a future terrain of terror operations (Branscomb, 2006: 108), which poses a significant threat to the UK's defence and security within the next 25 years.

Coker (2008) suggests that ethics is centred around how we should conduct relations with others and when codified by the state they transform into laws. Whilst Western forces debate ways of making 4 micro drones and exoskeletons ethically compatible, terrorists have no such concerns, which makes their terror operation more hostile without any consideration of ethics (Quintana, 2008: 11). Terrorists aim to create a violent spectacle, where ethics are non-existent, whereas militaries such those of the UK are faced with a deeper conundrum of how to operate such technologies in the most ethical ways (Quintana, 2008: 13). The troubling questions of whether such use of technologies can create fewer civilian casualties and collateral damage, and whether the proportionality be improved must be considered. Fundamental just war principles need to be adjusted to address the ethical and moral dilemma of future military operations using advanced technologies such as micro drones and exoskeletons. If military technologies such as micro drones and exoskeletons can fall freely into the hands of terrorists the consequences will be catastrophic, directly threatening the UK's defence and security over the next 25 years.

Advanced Missiles

The use of AI and nuclear weaponry in combination is not a novelty (United Nations University, 2018), but combining the two makes for a highly dangerous combination, with destabilising effects. States such as Russia are already developing AI missiles to dominate the new arms race (Tass, 2017). In a few years, Russia will create an AI powered missile range, including cruise missiles with elements of AI which will enable them 'to analyse the air and radar situation and make decisions on the altitude, the speed and the direction of their flight' (Tass, 2017). China is likewise expanding their efforts in AI, developing autonomous weapons which contribute toward existing research and development of unmanned systems and missile technology (Kania, 2020). China and Russia use fire-and-forget missile systems which are predominantly autonomous, pushing the human coordinator completely out of the loop (Scharre, 2018: 326-329). With Russia and China striving to develop advanced missiles that use AI, the UK will experience a direct threat to its defence and security over the next 25 years. What if covert developments of such advanced missiles by Russia and China overpower and outsmart those of the UK? This threat is severe, which will be one of the key areas in which the UK must sustain deterrence in order to keep up with its main rivals, whilst strengthening defence and security.

Terrorist groups such as ISIS and Hezbollah already use surface-to-air fired missiles (UNODC, 2021), making their operations highly lethal and destabilising. With the rapid advancement of AI and advanced weaponry becoming more readily accessible to terrorist groups, the threat is increasing and will likely develop into a major concern for the UK. The terrorists' fascination with autonomous weapons increases fears of them possessing advanced missiles in the future. If this happens, terrorist groups will become more lethal, meaning that the UK must be prepared

to strengthen counter-terrorism commitments as this will be one of the major threats to the UK's defence and security in the coming years.

Autonomous weapons such as advanced missiles create a difficult ethical dilemma. The possibility of launching completely autonomous missiles, 'capable of complex, far-raging reconnaissance and attack missions' (DARPA, 1983: 1) creates an ethical problem as the human is out of the loop during the operation. The key concern is that lethal autonomous weapon systems support extrajudicial killings, removing accountability away from humans and make killings more likely (Lin et al., 2008: 73-86). This problem will be exacerbated if access to such weapons becomes easier, reducing the accountability of the operator and increasing the probability of their use. Autonomous weapons could make the identification and persecution of active agents more challenging, which is a form of a 'retribution gap' (Danaher, 2016). This creates an ethical dilemma to be tackled, to make the use of such weaponry more ethical.

Cyber Operations

Cities can be virtual and bombs within them are highly destructive, making cyberwarfare a war of the future. Future attacks which the UK will endure will be predominantly in the cyber domain. This is already happening in espionage, sabotage and subversion (Rid, 2013) in states such as Russia and China, with an aim to disrupt the inner architecture of the UK state and cause catastrophic disruption to pursue their national interests. With advancements in AI in the cyber domain there will be further threats from state actors such as Russia and China. Russia's long history of election and referendum mingling more recently using cyber capabilities in particular targeting the UK, are indicative of the future cyber threat which the UK could be faced with by Russia. After potential Russian interference in the Scottish and Brexit referendums in the UK (Ellehuus et al., 2020), then with the next cyber acts of direct interference into the US 2016 elections (Abrams, 2019), the next major attack within the UK by Russia is not beyond the horizon. It will certainly happen within the next 25-year period or even multiple cyber bombs can be launched synchronically. The launch of Chinese global cyberattack put a direct threat toward the UK, as the 'telecoms, tech and governments' (Foreign, Commonwealth & Development Office et al., 2020) were under malicious attacks.

IoT 'refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data' (Ranger, 2020). A great fundamental transformation 'is the imminent physical results of cyber threats as IoT technologies enable closer interaction between humans and information systems' (Karabacak et al., 2017: 1). When IoT is being misused by terrorist groups like ISIS and Hezbollah for purposes of cyberterrorism, it can lead to a catastrophic consequence to which the UK needs to adapt faster and be more resilient to strengthen its defence and security when responding to such severe threat posed over the next 25 years. It is apparent that IoT applications are necessary 'to be deeply assessed as terrorists may attack then with easy-to-implement cyberattacks for the purpose of creating physical harm' (Karabacak et al., 2017: 1). This can be easily applicable to classify as a severe threat to the UK, as being part of the developed nation IoT is becoming easily accessible and terror groups

will utilise their holistic tactics to cause great destruction not only to UK state's infrastructure, but more significantly its citizens lives.

Russia and China's cyber activity towards the UK over the course of the next 25 years will continue to be 'ethically questionable' (Public-Private, 2019: 5). Existing international law and outdated Just War Theory do not apply straightforwardly to cyberwarfare (Dipert, 2010: 384), nor terrorists' use of IoT networks. This exacerbates the ethical dilemma of how to punish attackers, not only because tracing them is challenging, but also because the legal and ethical framework is inadequate. With advances in AI automation, the greater concern will be how a machine which generated an attack or launched a cyber bomb can be responsible for the destruction and disruption of the targeted state. It will be a challenge to develop a framework to punish actors for majorly covert cybercrime and terror over the next 25 years. The UK must build a more resilient technological infrastructure to minimise the risk and harm of such attacks, thus strengthening its defence and security.

Conclusion

Emerging technologies are integrating with AI systems to enable new threats to emerge. This will be the case within the next 25 years, as state actors such as Russia and China as well as terrorist groups such as ISIS and Hezbollah will exploit technologies in their strategic interests to dominate and overpower rivals including the UK. Discussion on micro drones, exoskeletons, advanced missiles and hostile cyber operations by both state and terrorist groups indicate that the exploitation of their advanced capabilities will continue to pose a severe threat to the UK. Joined technologies such as micro drones and exoskeletons, which are in development by Russia, create an almost Sci-Fi vision of future aggression which the UK may be faced with, requiring the UK to compete with Russia and China to be more resilient and guard its defence and security. Autonomous weapons such as advanced missiles have been shown to be highly destructive and different ranges will be more readily available to terror groups will generate a greater threat to the UK in the future. The cyber domain, coupled with IoT, will enable continued destruction and disruption by both state actors and terrorist groups. Ethical concerns are challenging when considered in relation to the use of such technologies by state and terrorist aggressors within the UK. These threats are critical and must be adequately addressed to enhance peace and security and protect the UK nation.

Bibliography

Abrams, A., 2019. Here's What We Know So Far About Russia's 2016 Meddling [WWW Document]. URL https://time.com/5565991/russia-influence-2016-election/ (accessed 9.5.21).

BBC, 2018. Russian Spy Poisonings: What We Know So Far [WWW Document]. URL https://www.bbc.co.uk/news/uk-43315636 (accessed 8.5.21).

Branscomb, L.M., 2006. Safety and Security in Megacities, in: Countering Urban Terrorism in Russia and the United States: Proceedings of a Workshop. Harvard University, pp. 1–256.

Bunker, R.J., 2015. 'Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications.' PA: Strategic Studies Institute 1–55.

Coker, C., 2008. Ethics and War in the 21st century, LSE international studies. Routledge, London; New York.

Danaher, J., 2016. 'Robots, Law and the Redistribution Gap.' Ethics Inf Techno 18, 299–309.

Defence Advanced Research Projects Agency Arlington VA, 1983. Strategic Computing. Next-Generation Computing Technology: A Strategic Plan for Its Development and Application to Critical Problems in defence [WWW Document]. URL https://apps.dtic.mil/docs/citations/ADA141982 (accessed 9.5.21).

Dipert, R.R., 2010. 'The Ethics of Cyberwarfare.' Journal of Military Ethics 9, 3384–410.

Ellehuus, R., Ruy, D., 2020. did Russia Influence Brexit? [WWW Document]. URL https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit (accessed 9.5.21).

Foreign, Commonwealth & Development Office, 2020. UK Warns of Chinese Global Cyber Attacks [WWW Document]. URL https://www.gov.uk/government/news/uk-warns-of-chinese-global-cyber-attacks

Harari, Y.N., 2019. 21 Lessons for the 21st Century.

Kania, E.B., 2020. "AI weapons" in China's Military Innovation [WWW Document]. Brookings. URL https://www.brookings.edu/research/ai-weapons-in-chinas-military-innovation/ (accessed 9.5.21).

Karabacak, B., Balogun, M., Bahsi, H., 2017. 'Preliminary Analysis of Cyberterrorism Threats to Internet of Things (IoT) Applications.' Franklin University 1–12.

Konaev, M., Bendett, S., 2019. Russian AI-Enabled Combat: Coming to a City Near You? [WWW Document]. War on the Rocks. URL https://warontherocks.com/2019/07/russian-ai-enabledcombat-coming-to-a-city-near-you/ (accessed 8.5.21).

Lin, P., Bekeley, G., Abney, K., 2008. Autonomous Military Robotics, Risk, Ethics, and Design (Ethics No. 1.0.9). United States.

Pecotlc, A., 2019. Whoever Predicts the Future Will Win the AI Arms Race [WWW Document]. Foreign Policy. URL https://foreignpolicy.com/2019/03/05/whoever-predicts-the-future-correctly-willwin-the-ai-arms-race-russia-china-united-states-artificial-intelligence-defense/ (accessed 8.5.21).

Pledger, T.G., 2021. The Role of Drones in Future Terrorist Attacks (Foreign Affairs No. 137). The Association of the United States Army, United States.

Public-Private, 2021. Communication of Cyber Capabilities: A Grand Cyber Arms Bazaar (Cyber Warfare). Public-Private Analytical Exchange Programme.

Quintana, E., 2008. The Ethics and Legal Implications of Military Unmanned Vehicles (International Affairs). BCS, United Kingdom.

Ranger, S., 2020. What is the IoT? Everything you Need You Know About the Internet of Things Right Now [WWW Document]. ZDNet. URL https://www.zdnet.com/article/what-is-the-internet-ofthings-everything-you-need-to-know-about-the-iot-right-now/ (accessed 9.5.21).

Rid, T., 2013. Cyber War Will Not Take Place. Hurst & Company, London.

Scharre, P., 2019. Army of None: Autonomous Weapons and the Future of War. W.W. Norton & Company, New York.

Tass, 2017. Russia to Develop Missiles Based on Artificial Intelligence [WWW Document]. URL https://tass.com/defense/957049#:~:text=Russia%20will%20roll%20out%20artificial,Boris%20Obnosov%20said%20on%20Thursday.&text=when%20it%20is%20possible%20to,where%20fun damental%20research%20is%20required. (accessed 8.5.21).

United Nations University, 2018. AI & Global Governance: AI and Nuclear Weapons - Promise and Perils of AI for Nuclear Stability [WWW Document]. URL https://cpr.unu.edu/publications/articles/ai-global-governance-ai-and-nuclear-weaponspromise-and-perils-of-ai-for-nuclear-stability.html (accessed 8.5.21).

UNODC, 2021. Conventional Terrorist Weapons [WWW Document]. URL https://www.unodc.org/images/odccp/terrorism_weapons_conventional.html (accessed 9.5.21).

World Economic Forum, 2018. Drone Terrorism is Now a Reality, and we need a plan to counter the threat [WWW Document]. URL https://www.weforum.org/agenda/2018/08/drone-terrorism-isnow-a-reality-and-we-need-a-plan-to-counter-the-threat/ (accessed 8.5.21).

Young, C., 2020. Russian “Sotnik” Combat Gear Allows Control of Micro-Drone Swarm [WWW Document]. Interesting Engineering. URL https://interestingengineering.com/russian-sotnikcombat-gear-allows-control-of-micro-drone-swarm (accessed 8.5.21).

Zhen, L., 2021. Chinese Military Micro Drone Unveiled at Abu Dhabi Weapons Show [WWW Document]. South China Morning Post. URL https://www.scmp.com/news/china/military/article/3123801/chinese-military-micro-droneunveiled-abu-dhabi-weapons-show (accessed 8.5.21)

Essay Title: Sensemaking, systemic competition, and the social compact

Author: Neil Ashdown[67]

Institute: Royal Holloway University

Abstract

The UK faces a growing range of complex transnational threats and is engaged in systemic competition with authoritarian states. This essay argues that the UK government's response to these threats should make a virtue of the country's values of openness and transparency. I argue that the UK government should support the development of sensemaking capabilities across society; that it should encourage the work of independent organisations that exploit the vulnerabilities inherent in authoritarian states; and that it should be more transparent about its own activities to preserve its social compact with the UK public.

Introduction

The Integrated Review set out the growing range of threats facing the UK over the next quarter century[68]. Underlying this analysis was a recognition that the UK will have to confront threats that it cannot deter or defeat, including pandemics, climate change, and great power competitors. This recognition coincides with an inflection point in UK defence and security strategy. The additional £16.5 billion in funding for the Ministry of Defence announced in November 2020[69] has filled the longstanding gap in the Ministry's finances. Past investment, including in the intelligence agencies and cyber, has laid the groundwork for the capabilities the UK will need in the future[70].

If this is not quite a clean slate for reassessing the UK's approach to the threats and opportunities of the 21st century, it is likely to be the cleanest slate that can be expected over the next 25 years.

Given this opportunity, the UK should focus on adapting its approach in three key areas: sensemaking, systemic competition, and the social compact. Failure to adapt in these areas represents the greatest threat to the UK's defence and security that it is within government's power to address. They are also areas where the UK has a comparative advantage if it can align its approach to defence and security with its wider societal values of openness and transparency.

---

[67] Centre for Doctoral Training in Cyber Security for the Everyday, Royal Holloway University of London (neil.ashdown.2019@live.rhul.ac.uk)

[68] Great Britain and HM Government, Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969402/The_Integrated_Review_of_Security_Defence_Development_and_Foreign_Policy.pdf.

[69] 'PM to Announce Largest Military Investment in 30 Years', GOV.UK, accessed 12 May 2021, https://www.gov.uk/government/news/pm-to-announce-largest-military-investment-in-30-years.

[70] Joe Devanny et al., 'The National Cyber Force That Britain Needs?', 2021.

Sensemaking

The greatest challenge facing the UK defence and security apparatus in the next 25 years will be making sense of complex and dynamic threats and hazards. All other aspects of the UK's approach to national security follow from its ability to anticipate emerging threats. The scale of this challenge requires the sensemaking apparatus to expand beyond the intelligence community, including by making better use of open-source intelligence (OSINT).

Sir David Omand has highlighted the increasing importance of sensemaking in the work of the intelligence agencies[71]. During the Cold War, the UK government's intelligence requirements were centred on the Soviet Union. This task drew together intelligence's two specialities – the acquisition of secrets and the analysis of data – and made the agencies an indispensable source of insights for government.

Today, the UK government's conception of national security has broadened to encompass a growing range of threats and hazards – including climate change, epidemiological risk, financial crime, and cybersecurity[72]. In all these and other 'non-traditional' intelligence requirements, the acquisition of secret information is less important than making sense of complex data[73].

Already, the adoption of 'intelligence-led' approaches to tackling these challenges has led to the development of sensemaking capabilities across government[74], civil society[75], and the private sector[76]. These capabilities are focused on the analysis of complex – often unclassified – data to inform action. They do not require secret intelligence to function.

Moreover, government is not always best placed to address newer threats. For example, the private sector will often have better visibility into cybersecurity threats than the government[77]. Similarly, there are likely to be areas where the private sector has more advanced data analysis capabilities than government.

In such cases, government should not attempt to replicate these capabilities but instead integrate the products of this analysis into its own sensemaking processes. OSINT could be deployed in parallel with traditional intelligence disciplines, providing cues for sensitive collection methods that can then verify or amend open-source assessments.

---

[71] David Omand, How Spies Think: 10 Lessons in Intelligence (New York, NY: Penguin, 2020).
[72] Great Britain and HM Government, Global Britain in a Competitive Age.
[73] David T. Moore et al., 'Sensemaking for 21st Century Intelligence', Journal of Intelligence History 20, no. 1 (7 April 2020): 45–59, https://doi.org/10.1080/16161262.2020.1746143.
[74] 'Joint Biosecurity Centre', GOV.UK, accessed 12 May 2021, https://www.gov.uk/government/groups/jointbiosecurity-centre.
[75] Sean Aday and Steven Livingston, 'NGOs as Intelligence Agencies: The Empowerment of Transnational Advocacy Networks and the Media by Commercial Remote Sensing in the Case of the Iranian Nuclear Program', Geoforum, Themed Issue: The 'view from nowhere'? Spatial politics and cultural significance of highresolution satellite imagery, 40, no. 4 (1 July 2009): 514–22, https://doi.org/10.1016/j.geoforum.2008.12.006.
[76] JD Work, 'Evaluating Commercial Cyber Intelligence Activity', International Journal of Intelligence and CounterIntelligence 33, no. 2 (2020): 278–308.
[77] Shannon Vavra, 'NSA Cyber Director Discusses US Response, Approach to Apparent Espionage Operation', CyberScoop, 16 June 2021, https://www.cyberscoop.com/rob-joyce-nsa-cybersecurity-director-solarwindsauthorities-russia-espionage/.

The goal would be the creation of a stronger sensemaking ecosystem, combining the strengths of different actors. Government could encourage the adoption of analytic tradecraft developed within the intelligence community – for example by developing accredited training programmes in satellite imagery analysis[78], a key tool for OSINT. By improving the quality of OSINT, government could with greater confidence incorporate this material into its own assessments.

Systemic competition

The Integrated Review is clear that the UK is engaged in systemic competition with powerful state adversaries. UK defence discourse is preoccupied by its adversaries' asymmetric advantages in grey zone or hybrid warfare[79]. Similarly, authoritarian regimes are perceived as having advantages over the UK in the use of strategic deception and disinformation[80]. However, the UK's open society and commitment to transparency provides it with asymmetric advantages of its own.

Bellingcat's work exposing the activities of Russian military intelligence is a prime example of this dynamic[81]. Bellingcat can conduct these investigations because of the UK's tolerance of civil society activity. Authoritarian states such as China and Russia either censor or strongly deter the activities of such independent investigative organisations.

However, Bellingcat does not achieve such notable successes only because of the open environment in which it operates. Rather, it successfully exploits the corruption that prevails within states such as Russia. A hypothetical Russian organisation investigating the activities of the UK intelligence agencies would not be able to purchase passport details, vehicle registrations, and telephone records on the dark net, in the way that Bellingcat investigators can do in Russia[82].

This vulnerability is not something that the Russian state can address – corruption is integral to the Russian leadership's hold on power[83]. Similarly, for states such as Russia and China, the need to have visibility into the inner workings of their own societies runs contrary to the kind of information security measures needed to protect their citizens' data and privacy, such as strong encryption[84].

---

[78] Ben Loehrke et al., 'Ethical Decision Making with Geospatial and Open Source Analysis', Stanley Center for Peace and Security, 20 January 2020, https://stanleycenter.org/publications/the-gray-spectrum/.
[79] 'Into The Grey Zone: Exploring the Murky Evolution of Warfare', Sky News, accessed 12 May 2021, https://news.sky.com/story/into-the-grey-zone-exploring-the-murky-evolution-of-warfare-12184358
[80] 'Democracies Need to Re-Learn the Art of Deception', The Economist, 16 December 2020, https://www.economist.com/christmas-specials/2020/12/16/democracies-need-to-re-learn-the-art-of-deception.

[81] 'How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine', Bellingcat, 26 April 2021, https://www.bellingcat.com/news/uk-and-europe/2021/04/26/how-gru-sabotageand-assassination-operations-in-czechia-and-bulgaria-sought-to-undermine-ukraine/.
[82] 'Hunting the Hunters: How We Identified Navalny's FSB Stalkers', bellingcat, 14 December 2020, https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology/.
[83] Mark Galeotti, The Vory: Russia's Super Mafia (Yale University Press, 2018).
[84] Greg Austin, Cybersecurity in China: The Next Wave (Springer International Publishing AG, 2018).

In the language of the tech sector, these are features – not bugs – of authoritarian societies. The UK government could encourage civil society and other actors to exploit these features, for example through the public disclosure of more intelligence on adversary activities to cue up open-source investigations[85].

Recent academic work by Brendan Green and Austin Long[86] suggests that states in long-term peacetime competition may counterintuitively gain value from revealing their clandestine capabilities. Specifically, disclosing such capabilities is rational when those capabilities are not unique and when adversaries cannot develop effective counters.

Independent open-source investigations that exploit the vulnerabilities of adversary societies can play a similar role in the context of systemic competition. Their 'capabilities' are not unique, as indicated by the proliferation of investigative units inspired by Bellingcat's work[87]. More importantly, adversaries cannot counter the work of these organisations without fundamentally changing aspects of their political systems. This suggests that the UK has a strong interest in encouraging the work of such organisations.

The social compact

In contrast to the work of these independent organisations, many of the UK government's capabilities in the field of cyber and intelligence depend on secrecy for their effectiveness[88]. Revealing information about these capabilities could reduce or negate their effect.

However, as conceptions of national security have broadened[89], the range of issues that requires the active engagement of the public has increased[90]. Cybersecurity is the most visible example of a challenge that cannot be addressed solely by government, but which requires working with the private sector and the public.

This creates a growing tension: the government needs to maintain secrecy about its capabilities, even as it seeks to build trust and engagement with the public. As Omand has argued, there is a need for a "grand understanding" between government and the public[91] – elsewhere termed the

[85] Betsy Woodruff Swan and Bryan Bender, 'Spy Chiefs Look to Declassify Intel after Rare Plea from 4-Star Commanders', POLITICO, accessed 27 April 2021, https://www.politico.com/news/2021/04/26/spy-chiefsinformation-war-russia-china-484723.
[86] 20 Brendan Rittenhouse Green and Austin Long, 'Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition', International Security 44, no. 3 (1 January 2020): 48–83, https://doi.org/10.1162/isec_a_00367.
[87] Muyi Xiao, 'How We Tracked Secret Oil Deliveries to North Korea', The New York Times, 22 March 2021, sec. Times Insider, https://www.nytimes.com/2021/03/22/insider/north-korea-oil-supply.html.
[88] Erik Gartzke and Jon R. Lindsay, 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace', Security Studies 24, no. 2 (3 April 2015): 316–48, https://doi.org/10.1080/09636412.2015.1038188.
[89] Sharon L Caudle, 'National Security Strategies: Security from What, for Whom, and by What Means', Journal of Homeland Security and Emergency Management 6, no. 1 (14 January 2009), https://doi.org/10.2202/1547- 7355.1526.
[90] 24 David Omand, Securing the State (Oxford University Press, 2014).
[91] Omand.

"intelligence compact"[92] or the "social compact"[93]. As Omand describes it, "[t]he essence of the social compact model is that through open debate, Parliament and the public can come to accept [that] the secret parts of the state are necessary"[94].

The UK's position on offensive cyber is an example of an area where greater transparency is needed. The Integrated Review emphasises the UK's desire to be a "democratic, responsible cyber power"[95]. For the UK to be democratically accountable to its population for its strategy on offensive cyber, it must do more to explain its activities to the public.

UK government has provided some brief examples of the sorts of activities that it might conduct under the rubric of offensive cyber[96]. Declassified information has provided some further, unofficial insights[97]. However, much as in the United States[98], the extreme sensitivity with which the UK government treats cyber activity stymies a better-informed public debate.

Secrecy around the operational details of cyber and intelligence capabilities remains essential. The old threats persist, and secret intelligence will continue to provide insights that cannot be acquired in other ways. Indeed, given the challenges that big data, surveillance technology, and biometrics pose to the ability of intelligence officers to operate under cover, it is very likely that some intelligence functions will require even greater secrecy to be effective[99].

Nonetheless, the UK government could do more to outline the sorts of activities that it will conduct using its cyber capabilities, along with its rationale for why these activities are necessary and proportionate. This could start with analogies to historical practice around intelligence and covert action. GCHQ's promotion of its history, including activities at Bletchley Park in the Second World War and in more recent conflicts[100], provide a wealth of public material that could be the basis of such explanations.

The biggest threat to the social compact is any revelation that the government has been behaving contrary to its professed principles. Historically, it has taken painful events –

---

[92] Nigel Inkster, 'The Protecting State', Survival 52, no. 5 (1 October 2010): 203–9, https://doi.org/10.1080/00396338.2010.522106.
[93] David Omand and Mark Phythian, Principled Spying: The Ethics of Secret Intelligence (Oxford University Press, 2018).
[94] Omand and Phythian
[95] Great Britain and HM Government, Global Britain in a Competitive Age
[96] 'National Cyber Force Transforms Country's Cyber Capabilities to Protect the UK', accessed 12 May 2021, https://www.gchq.gov.uk/news/national-cyber-force
[97]'Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL', National Security Archive, 10 August 2018, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08- 13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.
[98] Jason Healey and Robert Jervis, 'Overclassification and Its Impact on Cyber Conflict and Democracy', Modern War Institute, 22 March 2021, https://mwi.usma.edu/overclassification-and-its-impact-on-cyber-conflict-and-democracy/.
[99] David V Gioe, '"The More Things Change": HUMINT in the Cyber Age', in The Palgrave Handbook of Security, Risk and Intelligence (Springer, 2017), 213–27.
[100] John Ferris, Behind the Enigma: The Authorized History of GCHQ, Britain's Secret Cyber Intelligence Agency (New York: Bloomsbury, 2020).

Snowden[101], the Spycatcher trial[102], the ABC trial[103]– to spur the UK government to greater transparency about the activities of the intelligence agencies. Government could get ahead of this curve on offensive cyber, and on its defence and security strategy more broadly.

The amount of damage that the next 'Snowden' does to the UK's defence and security will be proportional to the distance between the UK's words and its actions. By being transparent about the activities that it conducts in the name of national security, the UK can reduce the reputational damage that the next leak will cause.

Conclusion

These three areas present opportunities for the UK to capitalise on its comparative advantages. The UK could support the development of analytical capability across society and make greater use of OSINT to support its work; it could encourage the work of independent organisations that exploit the vulnerabilities inherent in authoritarian states; and it could be more transparent about its own activities to strengthen its social compact with the UK public.

The UK's state adversaries will not follow this approach. They will fiercely centralise sensemaking capabilities within government and the military, exert greater control over their own societies, and disingenuously profess positions that run contrary to their actions in the grey zone and online.

The UK cannot wish away these state competitors, any more than it can ignore the threats posed by climate change, pandemic diseases, or online criminality. Our only choice is how we approach security and defence in the 21st century.

The UK will not achieve better outcomes in its defence and security policies over the next 25 years by reproducing in miniature the strategies used by its adversaries. Rather, we should make a virtue of openness and transparency, building trust and partnerships between government, the private sector, and the public.

Bibliography

Aday, Sean, and Steven Livingston. 'NGOs as Intelligence Agencies: The Empowerment of Transnational Advocacy Networks and the Media by Commercial Remote Sensing in the Case of the Iranian Nuclear Program'. Geoforum, Themed Issue: The 'view from nowhere'? Spatial politics and cultural significance of high-resolution satellite imagery, 40, no. 4 (1 July 2009): 514–22. https://doi.org/10.1016/j.geoforum.2008.12.006.

[101] Jamie Collier, 'Getting Intelligence Agencies to Adapt to Life Out of the Shadows', Council on Foreign Relations, accessed 1 March 2021, https://www.cfr.org/blog/getting-intelligence-agencies-adapt-life-out-shadows.
[102] Christopher Andrew, The Defence of the Realm: The Authorized History of MI5 (Penguin UK, 2012).
[103] Richard James Aldrich, GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency (London: HarperPress, 2011)

Aldrich, Richard James. GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency. London: HarperPress, 2011.

Andrew, Christopher. The Defence of the Realm: The Authorized History of MI5. Penguin UK, 2012.

Austin, Greg. Cybersecurity in China: The Next Wave. Springer International Publishing AG, 2018.

Caudle, Sharon L. 'National Security Strategies: Security from What, for Whom, and by What Means'. Journal of Homeland Security and Emergency Management 6, no. 1 (14 January 2009). https://doi.org/10.2202/1547-7355.1526.

Collier, Jamie. 'Getting Intelligence Agencies to Adapt to Life Out of the Shadows'. Council on Foreign Relations. Accessed 1 March 2021. https://www.cfr.org/blog/gettingintelligence-agencies-adapt-life-out-shadows.

'Democracies Need to Re-Learn the Art of Deception'. The Economist, 16 December 2020. https://www.economist.com/christmas-specials/2020/12/16/democracies-need-to-relearn-the-art-of-deception.

Devanny, Joe, Andrew Dwyer, Amy Ertan, and Tim Stevens. 'The National Cyber Force That Britain Needs?', 2021.

Ferris, John. Behind the Enigma: The Authorized History of GCHQ, Britain's Secret Cyber Intelligence Agency. New York: Bloomsbury, 2020.

Galeotti, Mark. The Vory: Russia's Super Mafia. Yale University Press, 2018.

Gartzke, Erik, and Jon R. Lindsay. 'Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace'. Security Studies 24, no. 2 (3 April 2015): 316–48. https://doi.org/10.1080/09636412.2015.1038188.

Gioe, David V. '"The More Things Change": HUMINT in the Cyber Age'. In The Palgrave Handbook of Security, Risk and Intelligence, 213–27. Springer, 2017.

Great Britain and HM Government. Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy, 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/969402/The_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

Green, Brendan Rittenhouse, and Austin Long. 'Conceal or Reveal? Managing Clandestine Military Capabilities in Peacetime Competition'. International Security 44, no. 3 (1 January 2020): 48–83. https://doi.org/10.1162/isec_a_00367.

Healey, Jason, and Robert Jervis. 'Overclassification and Its Impact on Cyber Conflict and Democracy'. Modern War Institute, 22 March 2021. https://mwi.usma.edu/overclassification-and-its-impact-on-cyber-conflict-and-democracy/.

bellingcat. 'How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine', 26 April 2021. https://www.bellingcat.com/news/ukand-europe/2021/04/26/how-gru-sabotage-and-assassination-operations-in-czechiaand-bulgaria-sought-to-undermine-ukraine/.

bellingcat. 'Hunting the Hunters: How We Identified Navalny's FSB Stalkers', 14 December 2020. https://www.bellingcat.com/resources/2020/12/14/navalny-fsb-methodology/.

Inkster, Nigel. 'The Protecting State'. Survival 52, no. 5 (1 October 2010): 203–9. https://doi.org/10.1080/00396338.2010.522106.

Sky News. 'Into The Grey Zone: Exploring the Murky Evolution of Warfare'. Accessed 12 May 2021. https://news.sky.com/story/into-the-grey-zone-exploring-the-murkyevolution-of-warfare-12184358.

GOV.UK. 'Joint Biosecurity Centre'. Accessed 12 May 2021. https://www.gov.uk/government/groups/joint-biosecurity-centre.

National Security Archive. 'Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet War Against ISIL', 10 August 2018. https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil.

Loehrke, Ben, Laura Rockwood, Melissa Hanham, and Luisa Kenausis. 'Ethical Decision Making with Geospatial and Open Source Analysis'. Stanley Center for Peace and Security, 20 January 2020. https://stanleycenter.org/publications/the-gray-spectrum/.

Moore, David T., Elizabeth Moore, Seth Cantey, and Robert R. Hoffman. 'Sensemaking for 21st Century Intelligence'. Journal of Intelligence History 20, no. 1 (7 April 2020): 45– 59. https://doi.org/10.1080/16161262.2020.1746143.

'National Cyber Force Transforms Country's Cyber Capabilities to Protect the UK'. Accessed 12 May 2021. https://www.gchq.gov.uk/news/national-cyber-force.

Omand, David. How Spies Think: 10 Lessons in Intelligence. New York, NY: Penguin, 2020. ———. Securing the State. Oxford University Press, 2014.

Omand, David, and Mark Phythian. Principled Spying: The Ethics of Secret Intelligence. Oxford University Press, 2018.

GOV.UK. ‘PM to Announce Largest Military Investment in 30 Years’. Accessed 12 May 2021. https://www.gov.uk/government/news/pm-to-announce-largest-military-investment-in-30-years.

Vavra, Shannon. ‘NSA Cyber Director Discusses US Response, Approach to Apparent Espionage Operation’. CyberScoop, 16 June 2021. https://www.cyberscoop.com/robjoyce-nsa-cybersecurity-director-solarwinds-authorities-russia-espionage/.

Woodruff Swan, Betsy, and Bryan Bender. ‘Spy Chiefs Look to Declassify Intel after Rare Plea from 4-Star Commanders’. POLITICO. Accessed 27 April 2021. https://www.politico.com/news/2021/04/26/spy-chiefs-information-war-russia-china484723.

Work, JD. ‘Evaluating Commercial Cyber Intelligence Activity’. International Journal of Intelligence and CounterIntelligence 33, no. 2 (2020): 278–308.

Xiao, Muyi. ‘How We Tracked Secret Oil Deliveries to North Korea’. The New York Times, 22 March 2021, sec. Times Insider. https://www.nytimes.com/2021/03/22/insider/north-korea-oil-supply.html.

Essay Title: Tomorrow's Warfare- Threats and Opportunities.

Author: Edward Holland

Institute: University of Exeter

Abstract

Britain will face a number of security threats in the next twenty-five years. Three in particular warrant in depth consideration both in terms of analysis and opportunities to counter. Tackling disinformation through state-private sector cooperation and public education, countering rising Islamist extremism in Africa through a two-pronged approach and investment in R&D to limit the effects of technology that increased the vulnerability of Britain's nuclear deterrence.

The nature of war is enduring; however, its character is ever changing (Clausewitz, 1832).As clichéd as this may seem, it has never been more relevant then now. Over the next twenty-five years Britain will face many security challenges, ranging from conventional threats that have plagued states for centuries, through to the increasingly murky and shadowy world of 'Grey Zone Warfare'. This essay shall focus specifically on three such potential challenges, ranging from current low-level aggression to emerging and future threats that pose an existential risk. Possible solutions and opportunities arising from these shall be discussed. A highly topical and ongoing security challenge is the threat posed to the UK from the spread of disinformation from both state and non-state actors. Aimed at influencing individuals in order to divide, disrupt and cause instability, the spread of disinformation is a current and emerging threat aimed at weakening British society and institutions. Her Majesty's Government needs to formulate an approach to combat disinformation through a combination of public-private sector cooperation and educating the public on the threat posed and how to identify disinformation. A second and increasingly concerning situation which poses a challenge to national security is the increasing emergence of Islamist extremist violence in Africa. Weak and failing states, such as Mali, Libya, and Mozambique provide a safe haven for 'Islamic State' (IS) affiliates and IS inspired groups following the collapse of IS in most of the Middle East. This creates a direct threat to the UK due to increased flows of migrants and terrorist activity in the UK and destabilisation of the region. Britain should combat the rising Islamist insurgencies in Africa through a combination of conventional warfighting and training host states armed forces, helping to create a 'global Britain' and counter increasing Chinese influence on the continent. Finally, the increasing technological advancement in ballistic missile defence (BMD) and submarine detection poses a threat for Britain's continuous at sea deterrence and leaves Britain with questions around its second-strike ability. Without a capable nuclear deterrence, the UK is more exposed to aggression. Britain should lead the way in R&D into developing technology to counter this rise.

A current and significant threat Britain is facing and one which is set to increase is the spread of disinformation. This is considered a type of Grey Zone Warfare (GZW) affecting both the individual citizen and public and private sector business. The 'Grey Zone' is, as defined by the US Special Forces Command, 'competitive interactions among and within State and non-State

actors that fall between the traditional war and peace duality' (Kapusta, 2015). Whilst the spreading of disinformation is not a new phenomenon, it being used in numerous capacities throughout history in a strategic and political setting, the Soviet Union labelling it 'active measures' (Todd C. Helmus, 2018), the ease of doing so has never been so great. The increased globalisation and rise of social media have allowed disinformation or 'fake news' to be spread more easily and rapidly than ever before. This can take numerous forms, including fake documents, edited photos, conspiracy theories, fake websites and accounts and altered Wikipedia entries (Fallis, 2015).

Both state and non-state actors, particularly Russia, engage in global propaganda campaigns, which have a direct impact on Britain (Todd C. Helmus, 2018). For example, in 2018 a fake account pretending to be then Defence Secretary, Gavin Williamson, linked the chemical weapon poisoning in Salisbury to the Real IRA. Again in 2019 a fake document spread online thought to be originating from the Spanish security services, described a plot by hard-line anti Brexit campaigners to assassinate Boris Johnson (Harding, 2019). Both examples have been linked to the Russian State and represent the tip of the disinformation iceberg. Adversaries are using the spread of disinformation in an attempt to undermine British democracy. The aim is to plant ideas into an individual's mind that will ultimately then lead them to question, doubt and mistrust British institutions and leaders. Using disinformation to undermine the government's legitimacy and authority is a very real and present issue. The divisive nature of the false information seeks to enhance pre-existing cleavages within British society. Ultimately the spreading of disinformation undermines British institutions, fosters mistrust, and weakens British society socially and politically.

Her Majesty's Government's approach so far has been lacking in reach. The Covid-19 pandemic has seen the government work closely with social media companies in order to tackle the spread of antivaccine disinformation (Government, 2020). This increased government-civil cooperation must be continued after the pandemic to ensure private organisations take greater responsibility in countering the spread of disinformation on their sites. There is however a fine balance between security and civil liberty, care must be taken to avoid the appearance of eroding freedom of speech. Owing to disinformation existing mainly in the cyber domain, the importance of the human element has often been overlooked. Disinformation is aimed at the individual and so too should the policies to counter it. The government's RESIST tool kit is an important first step in helping individuals identify disinformation (GCS, 2019), however, more must be done to inform the general public of the threat. This lack of public knowledge of the treat facilitates its spread and influence upon a greater number of people. Educating the public, with the 'SHARE checklist' (Feikert-Ahalt, 2019), will limit the number of people influenced by disinformation. The institution responsible for educating the public must, owing to the divisive nature of disinformation, be either a non-political or cross-party organisation. To be successful it must increase its reach through advertisement campaigns, targeting schools and workplaces. Greater public knowledge and understanding of the use and threat of disinformation will help to counter its effects.

A current threat and one which will increase in the near future is the spread of Islamist extremism to African states. With the collapse of 'Islamic State' in Iraq and Syria, Islamist extremists are searching for a new front in which to continue their conflict, seen by the increase in prominence and activity of 'Islamic State in the Islamic Maghreb' and 'Islamic State of the Greater Sahara'. The Malian War and the ensuing insurgency by armed Islamist groups have added to the instability of the Sahel region that risks creating a hot bed of Islamist extremism that will spread to the Maghreb and further into Western Europe (Sengupta, 2021). The insurgency in Mozambique, which started in October 2017, is another example of IS capitalising on the instability, taking responsibility for attacks in July 2019 (Morier-Genoud, 2020) in order to continue their conflict. The severity of the issue is highlighted by the 'Global Terrorism Index' reporting that with IS expanding, seven of the top ten countries with increases in terrorism were in Sub-Saharan Africa (Institute for Economics & Peace, 2020). The UK cannot afford an unstable and insecure Africa, especially in the Maghreb and Sahel regions, as it will have a vast and direct impact on flows of terrorism and migrants to the UK given its close geographical proximity.

The 'Integrated Review' showed the government's commitment to increased security and its intent for a more 'global Britain' (HM Government, 2021). Combatting the rise of Islamist extremism in Africa is an opportunity to do both. The deployment of 300 British troops on the UN MINUSMA mission is a start. However, more must be done. Deploying British forces in a counter-insurgency role is aligned with the policy of the 'Integrated Review' of increased deployment of British forces. The counterinsurgency effort would see troops actively combat the insurgents through conventional warfighting, coupled with a commitment to training the host nation's security forces, mimicking Op Shader and Turus. Training African state's forces and the G5 Sahel Joint Force (Etrangeres, 2019) will not only help combat the rising insurgencies but aims to bring increased and lasting stability to the region and deny IS and their affiliates with new territory. Furthermore, this approach will increase diplomatic ties with key African states and further British influence. It also seeks to counter China's 'Belt and Road' initiative balancing Chinese dominance in the region (Huang, 2016).

Within the next twenty-five years global technological advancements could pose an existential threat to Britain by undermining its strategic nuclear deterrence. Numerous technological changes could limit the effectiveness of Britain's Continuous At Sea Deterrence. Ballistic missile submarines (SSBNs) rely on 'concealment', the opacity of the sea and ocean, in order to remain undetected (Press, 2017) and thus able to deliver an assured second strike. This premise relies on the water remaining 'opaque'; dispersing electromagnetic radiation and ensuring sound is difficult to detect, due to the relatively quiet nuclear powered SSBNs and the background noise of the body of water. During the next twenty-five years however, improvements in Magnetic Anomaly Detection, such as the range of SQUID sensors (Hambling, 2017), advancements in sensors range, cost and size will allow a greater number to be used, combined with Autonomous Underwater Vehicles (AUVs) and the reduction of 'biofouling', improving the sensors lifetime and robustness (Mendenhall, 2018). Technological improvements in sonar and maritime detection, over the next twenty-five years, will limit Britain's SSBNs ability to remain undetected.

The ever-emerging field of Artificial Intelligence (AI) could have series consequences for Britain's nuclear deterrence. AUVs coupled with the previously mentioned improvements in sonar and sensing technology could prove devastating to SSBN 'invisibility'. This would offer adversaries the ability to detect, track and potentially attack SSBNs, removing Britain's second-strike capability (Vincent Boulanin, 2020). The decreasing cost of producing AUVs is concerning as they have the potential to be manufactured and deployed on a huge scale, being able to cover vast swathes of ocean, or maintain a continuous presence in the vicinity of HMNB Clyde, evading countermeasures.

AI will also have consequences for Ballistic Missile Defence (BMD), enabling faster detection, early warning and targeting (Vincent Boulanin, 2020). Autonomous BMD systems would not only alter the detection, allowing for greater speed when calculating the target, but also the decision-making process, intercepting the missile faster than ever before. The emergence of hypersonic technology, championed by the US, Russia and China (Reif, 2018), also threatens to improve BMD by intercepting the missile earlier due to its increased speed, travelling between 5 000 km/h and 25 000 km/h (Ibid.). More autonomous BMD, using hypersonic technology, has the potential to defeat a British second strike during the Trident missile's flight. With the limited missile capacity of the Dreadnaught class SSBN and maintaining only one continuously at sea, the British deterrence is vulnerable to the enhanced BMD (Futter, 2015) over the next twenty-five years.

Britain must be at the cutting edge of research and development into AI and SSBN detection in order to gain a strategic advantage. Development of Britain's own systems to counter SSBNs will allow it to derive technology both to maintain the 'invisibility' of its own deterrence and to counter adversaries' equipment.

Increased globalisation, advancements in technology and the growing power of the internet and social media have created new threats, contributing to, to quote Clausewitz 'the changing character of warfare' (Clausewitz, 1832). This essay has highlighted and discussed three threats to British national security. Both currently and in the near future, all pose a risk to the UK within the next twenty-five years. The current use of disinformation by both state and no-state actors to destabilise and weaken Britain poses a huge threat. The UK must work alongside social media firms, increasing public and private sector cooperation whilst, most importantly, educating the targets of disinformation, the public, of the real danger and identifying disinformation. The emerging Islamist insurgencies on the African continent, destabilising the region and creating a hot bed of Islamist extremism, must be addressed. British armed forces should be deployed to counter the insurgencies through conventional warfighting and training nations' forces, consolidating the influence of 'global Britain'. Finally, the rise of AI, improving sonar and SSBN detection and BMD will threaten the effectiveness of Britain's strategic nuclear deterrence in the near future, posing an existential threat. The UK must champion research and development into these areas in order to gain a technological advantage over potential adversaries, whilst also observing ways to counter the emerging technology. Britain has historically been famed for fighting the previous war, now it's time to turn her gaze to the future.

Bibliography

Alwardt, C., 2020. US Missile Defence Efforts and Chinese Reservations in East Asia. Asian Affairs, 51(3), pp. 605-620.

Analytica, O., 2021. Jihadist violence in Sahel will persist in 2021. Expert Briefings.

Clausewitz, C. V., 1832.

Etrangeres, M. d. l. e. A., 2019. G5 Sahel Joint Force and the Sahel Alliance. [Online] Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-andnon-proliferation/crises-and-conflicts/g5-sahel-joint-force-and-the-sahel-alliance/ [Accessed 5th February 2021].

Fallis, D., 2015. What Is Disinformation?. Library Trends, 63(3), pp. 401-426.

Feikert-Ahalt, C., 2019. Government Responses to Disinformation on Social Media Platforms: United Kingdom. [Online] Available at: https://www.loc.gov/law/help/social-media-disinformation/uk.php#II [Accessed 22nd March 2021].

Futter, A., 2015. Trident Replacement and UK Nuclear Deterrence: Requirements in an Uncertain Future. RUSI Journal, 160(5), pp. 60-67.

Futter, A., 2016. War Games redux? Cyberthreats, US–Russian strategic tability, and new challenges for nuclear security and arms control. European Security, 25(2), pp. 163-180.

GCS, G. C. S., 2019. RESIST Counter Disinformation Toolkit. [Online] Available at: https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/RESIST-Counter-Disinformation-Toolkit.pdf [Accessed 22nd March 2021].

Government, H. M., 2010. Securing Britain in an Age of Uncertainty, The Strategic Defence and Security Review, London: s.n. Government, H. M., 2015. National Security Strategy and Strategic Defence and Security Review 2015, London: s.n.

Government, H. M., 2020. Social media giants agree package of measures with UK Government to tackle vaccine disinformation. [Online] Available at: https://www.gov.uk/government/news/social-media-giants-agree-package-ofmeasures-with-uk-government-to-tackle-vaccine-disinformation [Accessed 3rd March 2021].

Government, H. M., 2021. Global Britain in a Competative Age, The Integrated Review of Security, Defence, Development and Foreign Policy, London: s.n.

Hambling, D., 2017. China's quantum submarine detector could seal South China Sea. New Scientist , Issue 3140.

Harding, L., 2019. Russians ‘spread fake plot to assassinate Boris Johnson’ on social media. The Guardian, 22nd June.

Huang, Y., 2016. Understanding China's Belt & Road Initiative: Motivation, framework and assessment. China Economic Review, Volume 40, pp. 314-321.

Kapusta, P., 2015. The Grey Zone, North Carolina: US Army Special Operations Command.

Mendenhall, E. A., 2018. Fluid Foundations: Ocean Transparency, Submarine Opacity, and Strategic Nuclear Stability. Journal of Military and Strategic Studies, 19(1), pp. 119-158.

Morier-Genoud, E., 2020. The jihadi insurgency in Mozambique: origins, nature and beginning. Journal of East African Studies, 14(3), pp. 396-412.

Peace, I. f. E. &., 2020. Global Terrorism Index 2020: Measuring the Impact of Terrorism, Sydney: s.n.

Press, K. A. L. a. D. G., 2017. The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. International Security, 41(4), pp. 9-49.

Raineri, L., 2020. Explaining the Rise of Jihadism in Africa: The Crucial Case of the Islamic State of the Greater Sahara. Terrorism and Political Violence.

Reif, K., 2018. Hypersonic Advances Spark Concern. Arms Control Today, 48(1), pp. 29-30.

Sengupta, K., 2021. British troops begin missions in Mali amid Islamist insurgency. The Independant , 1st February.

Todd C. Helmus, E. a., 2018. Russain Social Media Influence; Understanding Russian Propaganda in Eastern Europe, Santa Monica: RAND Corporation.

Todd S. Sechser, N. N. &. C. T., 2019. Emerging technologies and strategic stability in peacetime, crisis, and war. Journal of Strategic Studies, 42(6), pp. 727-735.

Vincent Boulanin, e. a., 2020. The positive and negative impacts of AI on strategic stability and, Stockholm: Stockholm International Peace Research Institute.

Essay Title: A Call for Hyperopia: The Value of Long-Term Policymaking to National Security and Democracy

Author: Fearghal Hughes

Institute: University of Liverpool

Abstract

Technology is very much a part of our everyday lives. However, long-term government policy often lags far behind technological developments and is of growing concern with regard to the increasing threat from authoritarian regimes. There is therefore a need to develop strategies which align with the development of technology. In order to meet this moving target, UK policymakers must think with greater foresight if Britain is to maintain its core democratic values. The present essay discusses the future threats of: (1) more sophisticated and impactful disinformation campaigns and (2) cyberattacks preying on technological vulnerabilities in critical infrastructure.

To produce long-term solutions to these problems, the present paper suggests that the UK must: (1) focus on the inclusion of educational programmes such as media literacy skills in the national curriculum and (2) ensure technological sovereignty in British infrastructure. Taking these steps may mean that the UK is better able to deter the increasing threat of attacks on democracy and bolster national security for the next 25 years.

Despite the arrival of COVID-19, it would appear that the world is becoming a better place. Global life expectancy continues to rise (Wang et al., 2020) and global poverty continues to fall (Jolliffe and Prydz, 2021). Improvements in global living standards are largely due to technological advancements (Elmaghraby and Losavio, 2014; Pham et al., 2020), particularly those made in the last 20 years (Martínez-García, 2013). However, the exponential rate at which technology develops (Rosenbach and Mansted, 2018) makes it increasingly difficult for regulation and policy to keep up (Barlow, 2018). UK policymakers therefore face a growing challenge as they consider the rapidly evolving capabilities of technology.

How will democracy be threatened?

In theory, technology should facilitate transparent and effective democracy (Schuler, 2020). In fact, the opposite has happened: technological advancements have allowed those seeking to undermine democracy to wage low-cost but impactful political warfare (Polyakova and Boyer, 2018). Prevailing technologies have increased the pervasiveness and success of political warfare campaigns, as the '*internet of things*' (*IoT*) has allowed agents to have direct access to targets and enabled them to disguise their intent (Omand, 2018). Modern tactics include disinformation, cyberattacks, and political subversion, all of which share the same objective: to sow confusion and distrust (Polyakova and Boyer, 2018; Rosenberger and Gorman, 2020) in democratic processes and institutions (Paterson and Hanley, 2020). With the increasing reliance of democracies on new technologies (Rudner, 2013) and the rapid shift in technological capabilities, the threats to democracies merit ever-growing concern (Landon-Murray et al., 2019).

Tactics will only worsen over time as it becomes harder for both humans and technology to distinguish real from falsified audio, video, or online personalities. Authoritarian states like China and Russia have invested heavily in Artificial Intelligence (AI), with China's AI investment constituting 60% of global investment – the largest in the world (Wang and Zhang, 2020).

Although Russia lags far behind, it is still capable of becoming a leading nation in AI technology (Saveliev and Zhurenkov, 2020). The threat of political warfare is not only limited to the likes of China and Russia. These tools appeal to other authoritarian nations seeking to undermine democracy, and Western nations will come up against greater threats of disinformation as technology evolves and proliferates in the coming years (Paterson and Hanley, 2020; Polyakova and Boyer, 2018).

The 2017 *#MacronLeaks* disinformation campaign is one example. Russian intelligence agents were linked to fake Facebook personae created to spy on and spread disinformation about French presidential candidate Emmanuel Macron. They were also reported to be responsible for the leaking a series of emails from campaign officials prior to the election (Menn, 2017), including fake documents claiming that Macron had a secret offshore bank account (De Haldevang, 2017). However, the attempt failed – it neither interfered in the election nor divided the French public (Conley and Jeangène Vilmer, 2018).

Suggested solution: Media literacy skills

How then should the UK respond? One explanation for the failure of the *#MacronLeaks* attack is that critical thinking and healthy scepticism are embedded within French culture (Jeangène Vilmer, 2021). The French media environment consists predominantly of mainstream and critical sources and is largely free of tabloid-style outlets and the 'alternative' websites which are more likely to be found in the UK (Conley and Jeangène Vilmer, 2018). Additionally, disinformation is more likely to be believed when an individual lacks the ability to critically evaluate media information presented to them (Pennycook and Rand, 2019). The media literacy skills of the French public are likely to have been a valuable tool in combatting the *#MacronLeaks* disinformation campaign.

In a study by Vraga and Tully (2016), students were shown either a public service announcement (PSA) or not before viewing a political talk show. They were then asked to evaluate the talk show on its accuracy, credibility, and its informative capacity. Those who saw the PSA beforehand were better able to critically evaluate the talk show than those who did not see the PSA. Notably, the most significant effect was found in those who watched the PSA and had been taught news media literacy as part of their undergraduate course. The authors conclude: 'if students receive media literacy education in their classrooms, small "injections" of media literacy in their lives could help these individuals apply critical thinking skills more regularly' (p.450).

There is now a strong argument for nations to provide their citizens with media literacy skills so that they may critically appreciate their media environment (Anderson and Rainie, 2020; Ireton and Posetti, 2018). Vraga and Tully's (2016) study implies that such skills are most effective when taught in a modular way as opposed to singular sessions. Long-term media literacy interventions have also supported the idea of teaching those skills in institutional settings (Hobbs and Frost, 2003; Kamerer, 2013; Watson and Vaughn, 2006). Sustained investment in educational institutions may therefore be the solution to the ever-changing threat of media disinformation (Seger et al., 2020). Educational policymakers should also consider, in particular, the inclusion of media literacy skills as part of the national school curriculum to provide future generations with the ability to critically assess media information.

Importantly, this would champion the core democratic value of freedom of the media. The ability of democratic nations to respond to information attacks from authoritarian states is weakened as the very media freedoms which they seek to uphold fail to distinguish between information and disinformation. This allows those should they so wish, to exploit this opportunity, essentially unhindered in their proliferation of politically-damaging narratives. It is therefore inherently

problematic for a democracy to redact information in such a way that does not promote the very authoritarianism from which it is attempting to differentiate itself. Consequently, an asymmetry is created that puts democratic nations at a tactical disadvantage (Paterson and Hanley, 2020). If it equipped its citizens with media literacy skills, the UK would demonstrate that it does not have to respond to disinformation attacks by succumbing to the censorship of authoritarianism.

How will UK infrastructure be threatened?

Political warfare tactics will not just focus on disinformation. Future attacks on democracy will likely involve the targeting of critical infrastructure (Polyakova and Boyer, 2018). Western infrastructure is increasingly dependent on the *IoT* as cities increase their reliance on smart technology (Caragliu et al., 2011; Rosenbach and Mansted, 2018). Technological developments continually enable the networked use of infrastructure in areas such as finance, health, and transport (He et al., 2016; Wells et al., 2014) and if these new technological structures are not maintained or updated, weaknesses may soon arise that allow for their exploitation (Hemme, 2015; Stoddart, 2016).

An offensive targeting Western infrastructure may have a fictitious ring, but it is already reality in parts of Eastern Europe. In 2015, an orchestrated attack on Ukraine's electrical grid occurred that left over 200,000 without electricity on Christmas Eve. Hackers managed to circumvent password access and disable the electricity grid and backup generators, causing the biggest known cyberattack made on an infrastructure system to date (Whitehead et al., 2017). The Ukrainian government claimed that the attack was instigated by Russian intelligence group Sandworm, whose malware has since been detected in companies responsible for US infrastructure (FireEye, 2016). More concerning is that Ukraine's cyber-defence (firewalls, manual controls, two-factor authorisation and segmented access) was more secure than that of the US at the time (Greenberg, 2017). As it stands, Western nations are ill-prepared to respond to such an attack (Hennessey, 2017).

The Ukraine attack demonstrates the importance of addressing vulnerabilities of infrastructure, as technological structures must therefore employ better-designed systems and more extensive security technologies (Farrell and Schneier, 2018). It should come as some reassurance to learn that the UK was rated the most cyber-secure nation by the Global Cybersecurity Index (ITU, 2019) and the work of GCHQ in respect of the recent #*WannaCry* cyberattack by North Korea is a good example. However, this should not be taken for granted and long-term policy is needed to meet emerging issues (Cameron et al., 2021). In particular, the slowly evolving nature of climate change, global warming, and structural upkeep of infrastructure necessitate long-term development strategies to bolster the security of national infrastructure (Evans et al., 2020).

Suggested solution: Infrastructural sovereignty

Material infrastructure is required for democracy to function effectively, which itself requires maintenance (Schuler, 2020). For decades, the UK has relied on Foreign Direct Investment (FDI) in its infrastructure as a substitute for government expenditure (Inderst, 2017; Pollitt, 2002). FDI in Western infrastructure from emergent economies has increased in recent years, spearheaded by China (McKinsey, 2013). Foreign ownership (shareholding) of UK infrastructure is roughly 40% (Inderst, 2017) with the Chinese state owning sizable stakes in British transport, steel, water, oil and nuclear power (Eaton, 2020). While Pinsent Masons (2014) have predicted far larger investments in UK infrastructure from China over the next few years, a Sunday Times investigation published online on 2 May 2021 showed that Chinese investors had 'amassed a portfolio of UK businesses, infrastructure, property … worth nearly £135 billion, almost twice as much as was previously suspected'. The investments have taken place since 2019, even

though ‘relations between Britain and China have grown increasingly tense’ (Watts and Nimmo, 2021).

This leaves Britain vulnerable to foreign powers whose intentions may not match the national interests of the UK (Rudner, 2013). For example, there have been cases of Chinese FDI in Europe that have facilitated the transfer of critical technology to Chinese military and industrial complexes that in turn has allowed for the technological advancement of their authoritarian capabilities (Kratz et al., 2020). Chinese FDI often comes from state-owned banks and likely serves a greater political purpose, even with regard to seemingly benign investments (Miettinen, 2020). The true goal of Chinese FDI in Western infrastructure remains to be seen as investments in the UK boast very little economic benefit to Chinese investors (Pettis, 2019).

Profiting from the singular concessions of foreign investors such as China is therefore not in the interest of national security (Ferchen et al., 2018). Instead, in the interests of technological sovereignty and national security, public policy should be circumspect of foreign ownership (Morozov and Bria, 2018). The UK has only very recently strengthened its powers to screen foreign investment with the enactment of the *National Security and Investment Act 2021*. The enactment on 29 April 2021 is very late as Britain had been one of the few Western economies that did not have standalone FDI legislation. Australia, for example, enacted more rigorous powers over a year ago (Heim and Ribberink, 2021) and the UK’s new FDI policies remain worryingly ambiguous (Lai, 2021) – more must be done to ensure the technological sovereignty of Britain’s infrastructure and support the work of the DSTL in protecting Homeland Security.

Systems science may be able to help in the strategic design of technological infrastructure (Grafius et al., 2020). Due to growing urbanisation, the technological components of modern infrastructure are increasingly integrated in order to provide reliable and effective service (Amin, 2010). However, this means that the overall infrastructure is highly vulnerable to cyberattacks due to the uniformity and interdependence of its components (Helbing, 2013; Rinaldi et al., 2001). Homogeneity in technological infrastructure can therefore be exploited in targeted attacks (Armstrong et al., 2009). For example, the current market is inclined to cloud storage which weakens diversity. If nations were to instead take charge and adopt their own technological infrastructures, the resultant cyber-diversity would drastically reduce the potential threat of an infrastructural cyberattack (Forrest et al., 2013; Salamat et al., 2009). In turn, the security of other democratic nations would increase if the UK were to develop and invest in its own unique technological infrastructure. Systems science may therefore inform current infrastructure to ensure technological sovereignty and national security (Forrest et al., 2013).

The need for long-term policy

Arthur Koestler was conscious of the gulf between the development of new technologies and its governing policies. In his 1941 work *Darkness at Noon*, Koestler explains that ‘every leap of technical progress brings with it a relative intellectual regression of the masses, a decline in their political maturity’ (p.176). The greater strides in technological advancements have further emphasised his point 80 years later and will continue to do so. It is therefore in the interest of national security for long-term planning not only to be aware of future shocks such as disinformation campaigns, but also to be able to respond to complex issues (Cameron et al., 2021) such as increased foreign ownership of UK infrastructure.

Overall, the benefits of future technological innovations will far outweigh the risks when democratic freedoms are observed and safeguarded (Elmaghraby and Losavio, 2014). Britain currently has the technological advantage, but this will ebb over time (Polyakova and Boyer, 2018) as the business of maintaining the UK’s security proves an increasingly complex task over the next 25 years. If Britain is to prevent the future threats of mass disinformation

campaigns and infrastructure cyberattacks then democratic values must continue to inform policy (Landon-Murray et al., 2019). The present paper argues that this can be achieved through the inclusion of media literacy skills in the national curriculum and ensuring the technological sovereignty of Britain's infrastructure. Ultimately, the UK must prepare for the next move in political warfare by being far-sighted in its policymaking.

References

Amin, S.M., 2010. Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems. In *IEEE PES General Meeting*, pp.1-5. IEEE.

Anderson, J. and Rainie, L., 2020. *Many tech experts say digital disruption will hurt democracy*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digitaldisruption-will-hurt-democracy/

Armstrong, R., Mayo, J. and Siebenlist, F., 2009. *Complexity science challenges in cybersecurity*. Sandia National Laboratories SAND Report.

Barlow, M., 2018. Big Data Culture Gap: Technology Advancing More Quickly Than People and Processes. Retrieved from http://radar.oreilly.com/2013/09/big-data-culture-gap-technology-advancing-more-quickly-than-people-and-processes.html

Cameron, G., Dixon, J., and Alderwick, H., 2021. *How can policymakers plan better for the long term?*, pp.1-17. The Health Foundation.

Caragliu, A., Del Bo, C. and Nijkamp, P., 2011. Smart cities in Europe. *Journal of urban technology*, *18*(2), pp.65-82.

Conley, H. A. and Jeangène Vilmer, J. B., 2018. *Successfully Countering Russian Electoral Interference*. Center for Strategic and International Studies. Retrieved from https://www.csis.org/analysis/successfullycountering-russian-electoral-interference

De Haldevang, M. (2017). *Russia Is Really Doing Its Damnedest to Defeat Macron and Make Le Pen President of France*. Quartz.com. Retrieved from https://qz.com/977028/russia-is-doing-its-damnedest-to-defeat-emmanuel-macron-and-make-marine-le-pen-president-of-france/

Eaton, G., 2020. *China's ownership of UK assets exposes Britain's broken model*. The New Statesman. Retrieved from https://www.newstatesman.com/politics/economy/2020/07/china-s-ownership-uk-assets-exposes-britain-s-broken-model

Elmaghraby, A. S. and Losavio, M. M., 2014. Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, *5*(4), pp.491-497.

Evans, C., Godart, B., Krieger, J., Kovarik, J.B., Mimram, M. and Palhol, F., 2020. *Building Resilient Infrastructure Systems,* pp.42-51. T20 Policy Brief.

Farrell, H. and Schneier, B., 2018. *Common-knowledge attacks on democracy*. Berkman Klein Center Research Publication.

Ferchen, M., Pieke, F. N., van der Putten, F. P., Hong, T. and de Blécourt, J., 2018. Assessing China's influence in Europe through investments in technology and infrastructure. Four cases. Leiden Asia Centre. Retrieved from https://euagenda.eu/upload/publications/untitled-199742-ea.pdf

FireEye, 2016. *Cyber attacks on the Ukrainian grid: what you should know*. Retrieved from

https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyberattacks-ukrainian-grid.pdf

Forrest, S., Hofmeyr, S., and Edwards, B., 2013. *The Complex Science of Cyber Defense*. Harvard Business Review. Retrieved from https://hbr.org/2013/06/embrace-the-complexity-of-cybe

Grafius, D. R., Varga, L. and Jude, S., 2020. Infrastructure interdependencies: opportunities from complexity. *Journal of Infrastructure Systems*, *26*(4), p.04020036.

Greenberg, A., 2017. *How an Entire Nation Became Russia's Test Lab for Cyberwar*. Wired. Retrieved from https://www.wired.com/story/russian-hackers-attack-ukraine/

He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y. and Gabrys, B., 2016. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. *In: 2016 IEEE Congress on Evolutionary Computation (IEEE CEC), 24-29 July 2016, Vancouver, Canada*, pp.1015-1021.

Heim, I. and Ribberink, N., 2021. Between growth and national security in host countries: FDI regulation and Chinese outward investments in Australia's critical infrastructure. *AIB Insights*, *21*(1).

Helbing, D., 2013. Globally networked risks and how to respond. *Nature*, *497*(7447), pp.51-59.

Hemme, K., 2015. Critical infrastructure protection: Maintenance is national security. *Journal of Strategic Security*, *8*(3), pp.25-39.

Hennessey, S. 2017. Deterring Cyberattacks: How to Reduce Vulnerability. *Foreign Affairs, 96,* p.39

Inderst, G., 2017. UK Infrastructure Investment and Finance from a European and Global Perspective. *Journal of Advanced Studies in Finance-ASERS*, *8*(1), p.15.

Ireton, C. and Posetti, J., 2018. *Journalism, fake news and disinformation: handbook for journalism education and training*, pp.17-26. Unesco Publishing.

ITU, 2019. *Global Cybersecurity Index (GCI) 2018*. Geneva: ITU. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01-2018-PDF-E.pdf

Jeangène Vilmer, J. B., 2021. Fighting Information Manipulation: The French Experience. In *Disinformation and Fake News*, pp. 75-89. Palgrave Macmillan.

Jolliffe, D. and Prydz, E. B., 2021. Societal poverty: A relative and relevant measure. *The World Bank Economic Review*, *35*(1), pp.180-206.

Kamerer, D., 2013. Media literacy. *Communication Research Trends*, *32*(1), pp.4-25.

Koestler, A., 1941. *Darkness at Noon*. Reprint, Vintage Classics, 2020.

Kratz, A., Huotari, M., Hanemann, T. and Arcesati, R., 2020. Chinese FDI in Europe: 2019 update. *A report by Rhodium Group (RHG) and the Mercator Institute for China Studies (MERICS)*.

Lai, K., 2021. National security and FDI policy ambiguity: A commentary. *Journal of International Business Policy*, pp.1-10.

Landon-Murray, M., Mujkic, E. and Nussbaum, B. 2019, "Disinformation in Contemporary U.S. Foreign Policy: Impacts and Ethics in an Era of Fake News, Social Media, and Artificial Intelligence", *Public integrity, 21*(5), pp.512-522.

Martínez-García, E., 2013. Technological progress is key to improving world living standards. *Economic Letter, 8*(4), pp.1-4.

McKinsey, 2013. *Infrastructure productivity: How to save $1 trillion a year*. McKinsey Global Institute.

Menn, J., 2017. *Exclusive: Russia used Facebook to try to spy on Macron campaign - sources*. Reuters U.S. Retrieved from https://www.reuters.com/article/us-cyber-france-facebook-spies-exclusive/exclusive-russia-used-facebook-to-try-to-spy-on-macron-campaign-sources-idUSKBN1AC0EI

Miettinen, J., 2020. OPPORTUNITIES AND THREATS OF CHINESE FOREIGN DIRECT INVESTMENT IN FINLAND Case study of investments in the forest industry, technology industry, and transportation infrastructure. [Thesis] Savonia University of Applied Sciences.

Morozov, E., and Bria, F., 2018. *Rethinking the Smart City: Democratizing Urban Technology*. New York: Rosa Luxemburg Stiftung.

National Security and Investment Act 2021, c. 25. Retrieved from https://www.legislation.gov.uk/ukpga/2021/25/pdfs/ukpga_20210025_en.pdf

Omand, D., 2018. The threats from modern digital subversion and sedition. *Journal of Cyber Policy*, *3*(1), pp.5-23.

Paterson, T. and Hanley, L. 2020, "Political warfare in the digital age: cyber subversion, information operations and 'deep fakes'", *Australian journal of international affairs, 74*(4), pp.439-454.

Pennycook, G. and Rand, D. G., 2019. Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. *Cognition*, *188*, pp.39-50.

Pettis, M., 2019. *Does the UK Benefit From Chinese Investment?*. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/chinafinancialmarkets/79261

Pham, N. M., Huynh, T. L. D. and Nasir, M. A. 2020, "Environmental consequences of population, affluence and technological progress for European countries: A Malthusian view", *Journal of environmental management, 260*, p.110143.

Pinsent Masons, 2014. China Invests West. *Pinsent Masons and Cebr, London*.

Pollitt, M.G., 2002. The declining role of the state in infrastructure investments in the UK. *Private initiatives in infrastructure: Priorities, incentives and performance*, pp.67-100.

Polyakova, A. and Boyer, S.P., 2018. The future of political warfare: Russia, the West, and the coming age of global digital competition. *EUROPE*.

Rosenbach, E. and Mansted, K., 2018. Can democracy survive in the information age?. *Belfer Center for Science and International Affairs*.

Rosenberger, L. and Gorman, L., 2020. How Democracies Can Win the Information Contest. *The Washington Quarterly*, *43*(2), pp.75-96.

Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, *21*(6), pp.11-25.

Rudner, M., 2013. Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), pp.453-481.

Salamat, B., Jackson, T., Gal, A. and Franz, M., 2009, April. Orchestra: intrusion detection using parallel execution and monitoring of program variants in user-space. In *Proceedings of the 4th ACM European conference on Computer systems,* pp.33-46.

Saveliev, A. and Zhurenkov, D., 2020. Artificial intelligence and social responsibility: the case of the artificial intelligence strategies in the United States, Russia, and China. *Kybernetes, 50*(3), pp.656-675.

Schuler, D., 2020. Can Technology Support Democracy?. *Digital Government: Research and Practice*, *1*(1), pp.1-14.

Seger, E., Avin, S., Pearson, G., Briers, M., Ó Heigeartaigh, S. and Bacon, H., 2020. *Tackling threats to informed decision-making in democratic societies: Promoting epistemic security in a technologically-advanced world*. Alan Turing Institute. Retrieved from https://www.turing.ac.uk/sites/default/files/2020-10/ epistemic-security-report_final.pdf

Stoddart, K., 2016. UK cyber security and critical national infrastructure protection. *International Affairs*, *92*(5), pp.1079-1105.

Vraga, E. K. and Tully, M., 2016. Effectiveness of a non-classroom news media literacy intervention among different undergraduate populations. *Journalism and Mass Communication Educator*, *71*(4), pp.440-452.

Wang, H., Abbas, K.M., Abbasifard, M., Abbasi-Kangevari, M., Abbastabar, H., Abd-Allah, F., Abdelalim, A., Abolhassani, H., Abreu, L.G., Abrigo, M.R. and Abushouk, A.I., 2020. Global age-sex-specific fertility, mortality, healthy life expectancy (HALE), and population estimates in 204 countries and territories, 1950–2019: a comprehensive demographic analysis for the Global Burden of Disease Study 2019. *The Lancet*, *396*(10258), pp.1160-1203.

Wang, L. and Zhang, L., 2020. A quantitative text analysis of artificial intelligence industry policy in China. *Proceedings of the Association for Information Science and Technology*, *57*(1), p.e358.

Watson, R. and Vaughn, L. M., 2006. Limiting the effects of the media on body image: Does the length of a media literacy intervention make a difference?. *Eating disorders*, *14*(5), pp.385-400.

Watts, R. and Nimmo, J., 2021. *Revealed: how China is buying up Britain*. The Sunday Times. Retrieved from https://www.thetimes.co.uk/article/revealed-how-china-is-buying-up-britain-t7njdhhc5

Wells, L. J., Camelio, J. A., Williams, C. B. and White, J., 2014. Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, *2*(2), pp.74-77.

Whitehead, D. E., Owens, K., Gammel, D. and Smith, J., 2017, April. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, pp.1-8. IEEE.

Essay Title: Scientific Publishers: A Growing Threat to UK Security

Author: Jack Suitor

Institute: Wallace Lab

1. Introduction

Information in the UK is controlled by a small number of unregulated and profit-seeking companies. However, it is not only tech giants like Facebook or Twitter that pose a threat to UK security. Indeed, other companies are disseminating dangerous information without consequence, all while siphoning millions of taxpayers' money into corporate profits. These companies are scientific publishers, who exploit the academic sciences for profit. To preserve profits, the companies make scientific research expensive and inaccessible. In doing so, these companies deny citizens the access to vitally important research. Additionally, publishing companies are completely unregulated, resulting in the distribution of dangerous, poorly executed, or fraudulent research. Furthermore, the publication of illegitimate and dangerous information will only become easier over the next 25 years. This essay will highlight the growing threat of scientific publishing to UK security and **how** it can be addressed.

2. The Current State of Scientific Publishing

2.1. Why scientists publish

Academic scientists must share their research. In this way, other scientists can build upon their findings to advance knowledge and help the public. To share their discoveries, scientists publish articles in peer-reviewed journals [1].

A peer-reviewed journal aims to publish only scientifically robust articles. Peer reviewers are experts in a relevant field who give feedback on submitted publications. After taking this feedback into account, an editor employed by the journal decides whether to publish a given article. In theory, this system should only allow ethical and rigorous work to be published [1].

Scientists usually aim to publish their work in widely-read "high impact" journals. An impact factor of a journal is a value which relates to how frequently the journal's articles are cited, and a journal with a large "impact factor" is considered high impact [1]. Scientists are incentivised to publish in high impact journals. For example, the UK Research Excellence Framework (REF) rewards universities whose scientists produce highly cited work. Therefore, although impact factors are not directly considered by REF, scientists who publish in high impact journals are more likely to have their research ranked as "excellent" [2].

2.2 The publishing business model

Following peer review, an article is published online and in physical copies of the journal. However, journals make readers to pay high fees to access any of their articles. In the case of higher education, universities can access many articles by paying millions of pounds to access a bundle of journals owned by a single publisher. Ultimately, almost all scientific research is fenced behind a paywall, inaccessible to members of the public, scientists working in industry, journalists, and even the UK government. This is particularly backwards, as the government and taxpayers pay for much research [3,4].

Scientists and peer reviewers receive little-to-no benefit from the research being paywalled. Neither authors nor peer reviewers are paid for their work. In fact, authors submitting manuscripts often have to pay the journal publishing fees. Ultimately, this means that academic publishing is one of the most profitable businesses in existence [3,4]. A desire to maintain this profitable business model is now generating security threats.

2.3 Propagation of dangerous or illegitimate articles

Many journals publish research which could be considered dangerous if used with the malicious intentions. For example, the journal Nature Protocols has published an article on the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), the virus responsible for the Covid-19 pandemic. This publication provides step-by-step instructions for how to evolve deadly new variants of the virus. These instructions could be understood and repeated by anyone with an undergraduate degree in biology [5], meaning the publication could effectively provide instructions to potential bioterrorists. Despite these risks, Nature publishing group decided to publish the paper because it is attention-grabbing and topical, meaning it will likely be highly-cited and help maintain Nature Methods' high impact factor. Because academic publishers are unregulated, Nature Methods could publish this information without seeking any external approval [1].

The study published in Nature Methods was scientifically legitimate, even if the results should not be accessible to a wide audience. However, now many "predatory journals" are publishing completely illegitimate articles. A predatory journal is a scientific publisher that claims to perform peer review but will actually publish anything submitted if a fee is paid by the authors. Because predatory journals are willing to publish anything, they often disseminate invalid research. Alarmingly, the number of predatory journals is substantially increasing, and will likely continue to increase over the next 25 years [6,7].

3. Threats to UK security posed by publishers

3.1 Spread of misinformation

The misinformation published by predatory journals poses a threat to UK security. For example, predatory journals have published articles making unsubstantiated claims that 5G could spread Covid-19 [8, 9]. Although these publications are illegitimate, it can be difficult to identify them as such. Predatory journals have official-sounding names and some are even archived in public databases, and, usually, only experts can distinguish predatory journals from legitimate sources [7]. As a result, dangerous publications can give a veneer of legitimacy to conspiracy theories. The spread of this misinformation poses a threat to UK security, as illustrated by attacks on and vandalization of 5G towers [10].

3.2 Availability of dangerous information

Even legitimate journals can publish dangerous articles. Examples include multiple publications detailing the nucleic acid and protein sequences of the H5N1 bird flu and the Spanish influenza viruses [10]. As such, malicious actors now have access to all the information required to resurrect and engineer a biological entity capable of being used as a deadly weapon. In other words, scientific publishers put UK security at risk to benefit their own profits. In some cases, governmental agencies advise publishers about whether an article should be published, however, journals have no legal obligation to comply with this guidance [11].

3.3 Diversion of resources away from legitimate threats

SciHub is a website that lets anyone illegally bypass the paywalls of academic journals to access publications. Despite its illegality, many scientists support SciHub because it makes science accessible [12]. SciHub has been labelled a security threat because of speculation that SciHub hacks universities to access research articles and putative links between SciHub's founder and Russian intelligence [13]. However, there is no evidence linking SciHub to any intelligence organisation nor proof that SciHub exists for any purpose other than to bypass journal paywalls [13]. Furthermore, it is unclear why shutting down SciHub would deter hacking, as universities can be hacked with or without the existence of SciHub.

Governmental security organisations appear to have been misled by academic publishers who are usually responsible for the publications of these allegations against SciHub [13]. As a result, UK and US governments have opened investigations into SciHub [13, 14]. Therefore, security organisations are effectively being misled and misallocating resources because scientific publishers wish to protect their paywalls. However, it is the unregulated publishers themselves who pose the legitimate risk to UK security.

4. Anticipated Trends in Scientific Publishing

4.1 Scientific research will become more accessible

Fortunately, some problems with scientific publishing are being addressed. Notably, publishing giants like Springer Nature have committed to having open access options for all of their journals [15]. As a result, the public will have greater access to scientific literature over the next 25 years. These changes have been forced by the enactment of "Plan S" and similar initiatives, which are driven by scientists and funding organisations who demand that all publicly-funded research is free to access [16]. By giving more people access to primary research, much misinformation can be combatted and fact checked. Therefore, scientists and funding bodies have helped combat the security threat posed by publishers.

4.2 The rise of alternative publications

It is not always efficient to distribute scientific research through peer-reviewed academic journals. This is because traditional publishing is a slow and arduous process that can even take years [1]. This is a serious problem during emergencies, for example, the Covid-19 pandemic. To address concerns like this, scientists use BioRxv, an alternative way to rapidly publish research. BioRxv is a service that publishes "preprints", articles that have not yet been peer-reviewed that are published immediately after submission and are free to access. Over the next 25 years, millions of preprints will be posted using BioRxv [17].

BioRxv poses a potential security risk. Recently, there have been multiple cases of inaccurate articles being published on the website throughout the course of the pandemic [17]. Conversely, hundreds of legitimate research articles have been published on BioRxv throughout the pandemic, immediately giving scientists access to vital discoveries [17,18]. Commendably, BioRxv took steps during the pandemic to block further publications that were obviously poorly-researched or made extreme claims [19]. As a result, BioRxv is both beneficial and threatening to UK security. The recently implemented high standards of BioRxv will be crucial for UK security, given that BioRxv will have a growing influence on the publishing industry in the next 25 years.

4.3 Information overload will be a growing problem in academic science

There is an overload of scientific articles, and this problem will continue to grow in the next 25 years. Every day, thousands of research articles are published, and many academics sift through hundreds of articles daily. The number of articles published is also growing exponentially, meaning this problem will only get worse [20].

This overload of new information poses a risk to science and UK security. The more articles that are published, the fewer that are thoroughly scrutinised. This creates an environment where illegitimate research can be published even in legitimate journals. For example, a poorly-executed study claimed that hydroxylchloroquine was an effective Covid-19 treatment [20]. This study was not legitimate, but was published in a journal owned by publishing giant Elsevier. This gave the publication an appearance of credibility, even though it was eventually discredited by other investigations [21]. However, the existence of the publication had already threatened UK and global security. Innumerable resources were wasted on further clinical trials using hydroxychloroquine [22], and conspiracy theories were further fuelled by this illegitimate research. Alarmingly, Elsevier has not retracted the hydroxychloroquine study, and has even included it in a special collection of articles relevant to the Covid-19 pandemic [20].

In the case of hydroxychloroquine, at least further research addressed the dangers posed by the original article. However, with an ever-growing number of publications, much research regarding less topical subjects is simply never scrutinised. Perhaps then it is unsurprising that nearly 70% of scientists say they have been unable to reproduce the discoveries published by other scientists [23]. With decreasing scrutiny on individual articles, more poorly executed and dangerous studies will be published in the coming years.

5. Potential mitigation measures

The government can protect the UK from the threats posed by scientific publishers. Simply put, scientific publishers should be regulated. Any journal that publishes false or dangerous information should be face fines or, in the case of predatory journals, enforced closures. Note that such regulations would not infringe on free speech. Just like the rest of society, academic publishers do not have the right to put the public at risk by deliberately disseminating false information.

Additionally, an independent regulator should ensure that research posing a security threat is not published. Experts should work with the regulatory body, similarly how the scientific advisory committee has worked with the UK government throughout the Covid-19 pandemic. With the help of experts, the committee could recommend if certain articles should be blocked from publication entirely or put under embargo for a limited time. Once again, failure to comply with regulatory guidance should lead to sanctions towards offending journals. For example, this committee would likely have prevented the publication of the Nature Methods paper detailing how to evolve new SARS-CoV-2 variants.

The UK government should also invest in platforms that enable the responsible sharing of scientific research. BioRxv performs an important public service, but it has not always prevented the publication of dangerous articles. The UK government should provide funding to BioRxv so it has the resources to maintain the high ethical standards it has implemented after the start of the Covid-19 pandemic. If all preprints can be screened in a similar manner, BioRxv will no longer pose a relevant security risk to the UK. This strategy would help make science more accessible, ensure that legitimate science can be shared quickly, and prevent the publication of clearly illegitimate research.

Finally, the UK government must change the culture of academic science. For example, universities and researchers are consistently rewarded for publishing in high impact journals. However, scientists should be rewarded for research that benefits the public good, not attention-grabbing research that simply garners citations. Therefore, the UK government must reform how universities are assessed. In this way, the government will de-incentive practices that have caused scientific publishing to grow into a security threat.

6. Conclusion

Academic publishing will continue to pose a risk to UK security over the next 25 years. Currently, publishers can distribute misinformation, often giving it a veneer of legitimacy in the process. Problems are exacerbated by an academic culture that rewards “high-impact” articles. Predatory journals, BioRxv, and information overload mean it will become even easier to publish illegitimate research in the next 25 years. However, by implementing regulations on academic publishers, the UK can stop this security threat. In doing so, the UK government can facilitate scientific publishing that is open, ethical, and safe.

References

[1] Copes, B. & Phillips, A. (2014) Future of the Academic Journal, Second Edition. *Future of the Academic Journal, Second Edition*, 1-449.

[2] Government, U.K. (2020) *Index of revisions to the ‘Guidance on submissions’ (2019/01).* Web: Available online: https://www.ref.ac.uk/media/1447/ref-2019_01-guidance-on-submissions.pdf

[3] Lariviere, V., Haustein, S. & Mongeon, P. (2015) The Oligopoly of Academic Publishers in the Digital Era. *Plos One*, 10(6).

[4] Suber, P. (2012) Ensuring open access for publicly funded research. *British Medical Journal*, 345.

[5] Xie, X. P., Lokugamage, K. G., Zhang, X. W., Vu, M. N., Muruato, A. E., Menachery, V. D. & Shi, P. Y. (2021) Engineering SARS-CoV-2 using a reverse genetic system. *Nature Protocols*, 16(3), 1761-1784.

[6] Cukier, S., Helal, L., Rice, D. B., Pupkaite, J., Ahmadzai, N., Wilson, M., Skidmore, B., Lalu, M. M. & Moher, D. (2020) Checklists to detect potential predatory biomedical journals: a systematic review. *Bmc Medicine*, 18(1).

[7] Gunaydin, G. P. & Dogan, N. O. (2015) A Growing Threat for Academicians: Fake and Predatory Journals. *Eurasian Journal of Emergency Medicine*, 14(2), 94-96.

[8] Fioranelli, M., Sepehri, A., Roccia, M. G., Jafferany, M., Olisova, O. Y., Lomonosov, K. M. & Lotti, T. (2020) 5G Technology and induction of coronavirus in skin cells. *J Biol Regul Homeost Agents.* E-4 ed.

[9] Sturm, T. & Albrecht, T. 'Constituent Covid-19 apocalypses: contagious conspiracism, 5G, and viral vaccinations'. *Anthropology & Medicine*.

[10] Kelion, L. (2020) Coronavirus: 20 suspected phone mast attacks over Easter. *BBC News*. Available online: https://www.bbc.co.uk/news/technology-52281315

[11] Resnik, D. B. (2013) H5N1 Avian Flu Research and the Ethics of Knowledge. Hastings Center Report, 43(2), 22-33.

[12] Van Noorden, R. (2016) Nature's 10: ALEXANDRA ELBAKYAN: Paper pirate. *Nature.*

[13] McKenzie, L. (2020) Is SciHub Safe?, Available online: https://www.insidehighered.com/news/2020/01/17/universities-ignore-growing-concern-over-sci-hub-cyber-risk

[14] Coughlan, S. (2021) Police warn students to avoid science website. *BBC News.* Available online: https://www.bbc.co.uk/news/education-56462390

[15] Sakellaropoulou, R. (2021) Introducing open access options for Nature and the Nature research journals. Available online: https://www.springernature.com/gp/researchers/the-source/blog/blogposts-open-research/open-access-options-for-nature-and-the-nature-research-journals/18782320

[16] (2019) PLOS welcomes the revised Plan S guidelines. Available online: https://theplosblog.plos.org/2019/05/plos-welcomes-the-revised-plan-s-guidelines/

[17] Fraser, N., Brierley, L., Dey, G., Polka, J. K., Palfy, M., Nanni, F. & Coates, J. A. (2021) The evolving role of preprints in the dissemination of COVID-19 research and their impact on the science communication landscape. *Plos Biology*, 19(4).

[18] Brierley, L. (2021) Lessons from the influx of preprints during the early COVID-19 pandemic. *Lancet Planetary Health*, 5(3), E115-E117.

[19] Kwan, D. (2020) How swamped preprint servers are blocking bad coronavirus research. *Nature.* Available online: https://www.nature.com/articles/d41586-020-01394-6

[20] Van Noorden, R. (2014) Global scientific output doubles every nine years. *Nature*. Available online: http://blogs.nature.com/news/2014/05/global-scientific-output-doubles-every-nine-years.html

[21] Lagier, J. C., Million, M., Gautret, P., Colson, P., Cortaredona, S., Giraud-Gatineau, A., Honore, S., Gaubert, J. Y., Fournier, P. E., Tissot-Dupont, H., Chabriere, E., Stein, A., Deharo, J. C., Fenollar, F., Rolain, J. M., Obadia, Y., Jacquier, A., La Scola, B., Brouqui, P., Drancourt, M., Parola, P., Raoult, D. & Force, I. C.-T. (2020) Outcomes of 3,737 COVID-19 patients treated with hydroxychloroquine/azithromycin and other regimens in Marseille, France: A retrospective analysis. *Travel Medicine and Infectious Disease*, 36.

[22] Self, W. H., Semler, M. W., Leither, L. M., Casey, J. D., Angus, D. C., Brower, R. G., Chang, S. Y., Collins, S. P., Eppensteiner, J. C., Filbin, M. R., Files, D. C., Gibbs, K. W., Ginde, A. A., Gong, M. N., Harrell, F. E., Hayden, D. L., Hough, C. L., Johnson, N. J., Khan, A., Lindsell, C. J., Matthay, M. A., Moss, M., Park, P. K., Rice, T. W., Robinson, B. R. H., Schoenfeld, D. A., Shapiro, N. I., Steingrub, J. S., Ulysse, C. A., Weissman, A., Yealy, D. M., Thompson, B. T., Brown, S. M. & Natl Heart Lung Blood Inst, P. C. (2020) Effect of Hydroxychloroquine on Clinical Status at 14 Days in Hospitalized Patients With COVID-19 A Randomized Clinical Trial. *Jama-Journal of the American Medical Association*, 324(21), 2165-2176.

[23] Baker, M. (2016) 1,500 scientists lift the lid on reproducibility. *Nature*. Available online: https://www.nature.com/news/1-500-scientists-lift-the-lid-on-reproducibility-1.19970

Essay Title: Why open access information and the advancement of DNA synthesis is increasing the biosecurity threat to the United Kingdom.

Author: Nick Johnson

Institute: University of Edinburgh

Abstract

The acute risk of biological substances to public health and national security has never been higher. The recent severe acute respiratory syndrome coronavirus (SARS-CoV) and Ebola outbreaks have shown how rapidly an infectious disease can spread in a local setting, as well as globally, with devastating outcomes. Due to increased globalisation and deforestation, these potential pandemic events are also becoming increasingly likely through natural zoonotic transmission. However, due to the advent of genetic synthesis and engineering, humans have the capability to manipulate the genetic code of pathogenic viruses to increase, for example, transmissibility and mortality. Recent advancements in biotechnology are making genetic material easier to obtain and much cheaper. Even though these processes undergo screening and international agreements are signed by large-scale manufacturers, advanced technologies are making small-scale genetic synthesis by individual laboratoriesincreasingly viable. This createsthe potential for DNA to be synthesised withoutscreening and stringent regulation, in a capacity which global genetic material manufacturers forgo. Now information is freely available to anyone with an internet connection, due to open-access servers and the rise in popularity in of pre-print servers, making it possible to obtain DNA sequences without barriers. This combination of ease of access to information and advancing technology in genetic synthesisincreases the risk of these organisms being obtained and manipulated with malicious intent. Technological advancements should be welcomed and utilised, however, this creates a need for the United Kingdom (UK) to be vigilant and agile with the underlying threats they pose.

Introduction into Genetic Synthesis

Deoxyribonucleic acid (DNA) is composed of a double stranded polymeric chain of molecules called nucleotides, structured in a helical shape, and are present in all organisms (Crick and Watson, 1954; Alberts et al., 2002; Frazer et al., 2003) These DNA macromolecules code for protein synthesis and imperative for functionality and reproduction; and are unique to each organism. (Alberts et al., 2002) Viruses operate in much in the same capacity, however, can either contain DNA or ribonucleic acid (RNA) as genetic material. (Wolf et al., 2018) Genetic information is transferrable between different organisms and can be introduced to generate novel functionality. (Alberts et al., 2002; Khan et al., 2016; Kunjapur, Pfingstag and Thompson, 2018) Being able to efficiently synthesise genetic information makes it possible to be able to genetically modify organisms. (Ellis, Adie and Baldwin, 2011; Hughes and Ellington, 2017; Katz et al., 2018).

Recent advances in modern genetic synthesis have paved the way for an innovative and vibrant biotechnology industry. The importance of this technology has been highlighted most recently with the COVID-19 pandemic with the rapid development of RNA-based vaccines (van Doremalen et al., 2020). Other applications include strengthening the UK's commitment to a carbon neutral economy by shifting the reliance on the manufacture of high-value chemicals from petroleum-based feedstocks to a bio-based industry in which synthetic biologists and metabolic engineers can valorise renewable and waste feedstocks, such as simple sugars, in

living microorganisms. (Shears, 2019) Increased emphasis by industry on more sustainable processes have increased research in the area and made use of genetically modified strains of organisms. (Tang and Zhao, 2009; Singh, 2011) With technological advancements, such as the examples highlighted, this just gives a small illustration of the potential benefits of the ongoing development of genetic synthesis. This has the potential to significantly impact the UK, helping tackle many of the major long-term global issues and help the UK government achieve its commitment to net zero by 2050. (Delisi, 2019; Shears, 2019)

The Increasing Demand for Commercial Gene Synthesis

Due to efficiency and cost, the vast majority of genes are synthesised by major manufacturers based in the USA, Germany and China, using enzymatic methods. (Engels and Uhlmann, 1989; Casimiro, Wright and Dyson, 1997; Tucker, 2010) Due to the resources available to industry and having high throughput DNA synthesis technologies in place, prices per genes have dropped dramatically over the recent decades and now fall around 5% annually. (Carlson, 2018) This drive is making biotechnology more economically viable to invest in and there has been an increase in demand for gene synthesis as more research is going into the sector. (Kunjapur, Pfingstag and Thompson, 2018; Senior, 2020)

This expanding scientific community show a collaborative approach to freely sharing information and raw data, such as genetic sequences, through journal publications and open-access databases i.e. UniProt, leading to scientists being able to use each other's findings to aid their own research. (van Aken and Hammond, 2003) However, there is an element of trust, with the assumption that this information will be used ethically. (Teixeira da Silva and Dobránszki, 2015) Of concern is the misuse of genetic databases along with continually evolving literature on pathogenicity mechanisms and how different pathogens evade the human immune system. (Pearson, 2000; Fraser and Dando, 2001; Reding and Eaton, 2020) This increased knowledge can facilitate the development of biological weapons and pose a threat to the UK.

Protective Measures

The greatest concern is that synthetic DNA can be used to engineer a novel pathogen, resurrect a virus, such as smallpox, or modify an existing virus to increase mortality or transmissibility. (Tucker, 2010) Many viral/bacterial genetic sequences are freely made available through open access databases, therefore, entirely possible. In 2002, this was achieved by J. Cello and co-workers in the de novo synthesis of a cell-free infectious poliovirus and more recently, horsepox, by Noyce and co-workers. (Cello, Paul and Wimmer, 2002; Noyce, Lederman and Evans, 2018) Owing to their low lethality, these viruses would not be considered an effective bioweapon. However, it serves a reminder of the risks if repeated with a virus with a much higher mortality rate. (van Aken and Hammond, 2003)

As most genetic synthesis is conducted via major industry partners currently, this makes the ability to control and monitor the material being synthesised simpler. (Evans and Selgelid, 2015) Industry realised the biosecurity risks and the potential consequences, and are now monitoring all genetic material ordered through their platform. (Fischer and Maurer, 2010) Blue Heron Biotech, LLC was the first major gene synthesis company to put measures in place, using only verified customers and carrying out continuous screening of all orders for restricted DNA sequences. (Tucker, 2010) This has now been extended to the 6 leading companies in the sector forming the International Consortium for Polynucleotide Synthesis (ICPS) and in 2010, the United States Department of Health and Human Services published a screening framework

for genetic synthesis manufacturers. (Diggans and Leproust, 2019) The development of fast and reliable genetic sequencing detection software increases the ability to screen the vast number of orders that are being placed. Currently, a blackwatch software has been formulated to screen DNA being ordered relating to pathogenicity and enhances the biosurveillance of potentially harmful organisms. (Tucker, 2010)

However, these screening efforts would be in vain if the regulations are not enforced by governments on an international scale. Currently, measures are industry led and largely voluntary. Several international treaties are in place to restrict gene synthesis, however, there are several countries yet to promote ethical screening practices, including a global leader; China, also there are no meaningful verification procedures agreed with the Biological Weapons Convention (BWC) treaty. (Tucker, 2010; Kemp et al., 2021) Therefore, efforts need to be increased to encourage global cooperation in screening efforts to safeguard global biosecurity along with stricter legislation at government level.

Advancing Technologies

Leading gene synthesis companies are now using state of the art facilities and technologies to drive production rates and increase turnover. (Kosuri and Church, 2014; Hughes and Ellington, 2017) However, technologies are being developed to make it quicker and easier to synthesise genes. (Kosuri and Church, 2014) For example, typically in nature DNA synthesis requires DNA templates, however, an enzyme initially identified from the immune system of mammals (Motea and Berdis, 2010), terminal deoxynucleotidyl transferase (TdT), is able to add free nucleotides onto the end of sequences. (Bollum, 1962; Eisenstein, 2020) Recent work by S. Palluk et al. (2018) have been able to harness this enzyme to be able to add free nucleotides in a controlled manner with yields comparable to current synthesis techniques. (Palluk et al., 2018; Barthel et al., 2020) The potential for this technology is vast if optimised, as it can potentially create larger DNA strands (around 1 kb) which are currently inaccessible with existing chemical methods and paves the way for a new mass market of DNA printing, similar to a 3D-printer. (Eisenstein, 2020) As such, DNAScript®, have recently incorporated this TdT technology into a prototype benchtop DNA printer, indicating this will be commercially available within the next couple of years. (Perkel, 2019; EDS - DNA Script, 2021) The ability to inexpensively synthesise DNA quickly would enable start-up companies and smaller suppliers to gain a foothold in this industry, as well as eventually leading to individual laboratories being able to routinely synthesise genes on-site. There are many other companies also developing advanced DNA synthesis platforms. One such company, Evonetix®, are incorporating a designed silicon chip controlling the synthesis of DNA at different reaction sites in parallel by controlling the temperature to selectively deprotect strands of DNA before new bases are added. (Kirk, 2019) In 2020, Evonetix® agreed a collaboration with Analog Devices® to scale-up and manufacture devices for this technology to be able to go commercial with their desktop DNA writer. (Evonetix and Analog Devices Collaborate on Third-Generation DNA Synthesis Platform, 2020)

These examples highlight the rapid developments in this sector, driving growth in biotechnology research. However, there still needs to be caution and close monitoring from the UK biosecurity authorities of new DNA technologies coming to market. As DNA synthesis becomes more accessible, the regulation of gene manufacture will become increasingly problematic. (Wang and Zhang, 2019) Individual laboratories and smaller start-up companies will not have the same access to screening software and until stringent regulation of these expanded capabilities comes into law, this creates a potentialroute for illicit use and creates an opportunity for a black market in DNA synthesisto emerge.

The potential threat to public security

With the ongoing global COVID-19 pandemic costing countless lives and causing global economies to dramatically suffer, the UK has a first-hand account of how a biological threat can impact the world around us. A virus or another pathogenic species which has an increased mortality rate spreading globally should be of utmost concern. Evolving technology increases the capabilities to synthesise large DNA fragments and whole genomes of viruses and pathogens. (Cello, Paul and Wimmer, 2002; Kosuri and Church, 2014). As advancements in genetic synthesis make DNA/RNA more accessible, this makes bio-surveillance increasingly difficult as the network of manufacturers/distributors increase. This increases the likelihood that organised crime groups, terrorist organisations and outlaw states are able to obtain genetic material, posing a greater threat to national security. (Evans and Selgelid, 2015)

This threat is genuine as increasing tensions arise around the world with the rise of terrorist organisations and hostile autocratic regimes. The BWC states defensive bioweapon programmes are permitted (Leitenberg, 2003); however, this does not stop clandestine development of offensive bioweapons as not all countries in the world have signed and ratified this treaty. Current intelligence suggest that Russia, Syria, Iran, North Korea and China also have extensive state-sponsored bioweapons programs, some of which have links to terrorist organisations, which lack transparency in the international community. (Leitenberg, 2001; van Aken and Hammond, 2003; Pfluke, 2019).

Facing a threat of this magnitude, an international treaty is inadequate unless vigilant international monitoring procedures are undertaken. This threat will increase in the coming years with the development of accessible genetic material and evolving literature being made available. (Fraser and Dando, 2001) Therefore, the BWC treaty should be revisited and reviewed, and the UK should be agile to the threat and impose more stringent measures on monitoring domestic genetic synthesis and the import/export of such material worldwide.

Suggested Solutions

Moving forward, national and global governance needs to develop as DNA technology evolves, achieving a balance to facilitate the benefits alongside the increasing risk they pose. (Fraser and Dando, 2001; Kemp et al., 2021) As DNA synthesis capabilities expand, so will the companies and laboratories which have these capabilities, therefore, it is critical bio-surveillance is available to all developers and producers to promote good practice and minimise the increased risks. The information of said risks and national biosafety rules should also be effectively communicated to the scientific community to increase accountability of the individual laboratory.

Currently, bio-surveillance and monitoring policy is mostly set by the private sector, however if national and global biosecurity is to be maintained in this new dawn of biotechnology, governmental regulation will have to increase. (Fischer and Maurer, 2010; Kemp et al., 2021) Therefore, it should be of uppermost importance to government to promptly develop new policy and legislation. The nuclear threat initiative (NTI) is a non-profit global organisation which works towards increasing knowledge and awareness of the increase in biotechnological advancements and reducing the risk of biological material being misused. This organisation helps and encourages governments and the private sector to work collaboratively towards creating effective policies and frameworks to reduce this global threat. So more widely, working with the NTI, ICPS and the International Association of Synthetic Biology (IASB), the UK needs

to be a global leader in harmonising a new universal code of conduct in synthetic biology, which currently does not exist, and evolving strictly enforced monitoring mechanisms for developing new DNA synthesis technologies. (Fischer and Maurer, 2010)

Additionally, full international cooperation and enhanced global governance of any new mechanisms is required. (Roffey et al., 2002) Consequently, there needs to be further dialogue with states and stakeholders to implement any proposed rules and harsh sanctions to anyone who fails to comply. This should develop alongside new on-site verification procedures by the BWC. Such procedures would aim to minimise the risk of new DNA technologies but would need to be under constant review.

Conclusions

Biotechnological advancements underpin the future development of a greener economy and society. As a world leader in synthetic biology and biotechnology, the UK is at the forefront of advancements in the sector. However, this also requires the UK to lead the monitoring and surveillance of biological material. The advancements in DNA synthesis are making genetic material easily accessible and cheaper, which is driving innovative R&D at an unprecedented rate. However, as DNA synthesis becomes cheaper and more readily available, this makes it increasingly difficult to monitor DNA production and enables the potential for unregulated genetic material to be synthesised and distributed, posing a threat to public and global health and security. If the UK and the wider international community do not respond to these evolving biotechnological advancements, this could have devasting consequences to its citizens.

References

Van Aken, J. and Hammond, E. (2003) 'Genetic engineering and biological weapons. New technologies, desires and threats from biological research', EMBO Reports. European Molecular Biology Organization, 4, p. S57. doi: 10.1038/sj.embor.embor860.

Alberts, B. et al. (2002) 'The Structure and Function of DNA', in Molecular Biology of the Cell. 4th Ed. Garland Science. Available at: https://www.ncbi.nlm.nih.gov/books/NBK26821/ (Accessed: 27 April 2021).

Barthel, S. et al. (2020) 'Enhancing terminal deoxynucleotidyl transferase activity on substrates with 3′ terminal structures for enzymatic De Novo DNA synthesis', Genes. MDPI AG, 11(1), p. 102. doi: 10.3390/genes11010102.

Bollum, F. J. (1962) 'Oligodeoxyribonucleotide-primed Reactions Catalyzed by Calf Thymus Polymerase', The Journal of Biological Chemistry, 237(6), pp. 1945–1949. doi: 10.1016/S0021-9258(19)73964-7.

Carlson, R. (2018) 'Competition and the Future of Reading and Writing DNA', in Synthetic Biology. Weinheim, Germany: Wiley-VCH Verlag GmbH & Co. KGaA, pp. 1–13. doi: 10.1002/9783527688104.ch1.

Casimiro, D. R., Wright, P. E. and Dyson, J. (1997) 'PCR-based gene synthesis and protein NMR spectroscopy', Structure, 5(11), pp. 1407–1412. Available at: http://biomednet.com/elecref/0969212600501407 (Accessed: 27 April 2021).

Cello, J., Paul, A. V. and Wimmer, E. (2002) 'Chemical synthesis of poliovirus cDNA: Generation of infectious virus in the absence of natural template', Science. American

Association for the Advancement of Science, 297(5583), pp. 1016–1018. doi: 10.1126/science.1072266.

Crick, F. H. C. . and Watson, J. D. (1954) ‘The complementary structure of deoxyribonucleic acid’, Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences. The Royal Society, 223(1152), pp. 80–96. doi: 10.1098/rspa.1954.0101.

Delisi, C. (2019) ‘The role of synthetic biology in climate change mitigation’, Biology Direct. BioMed Central Ltd., 14(1), p. 14. doi: 10.1186/s13062-019-0247-8.

Diggans, J. and Leproust, E. (2019) ‘Next steps for access to safe, secure DNA synthesis’, Frontiers in Bioengineering and Biotechnology. Frontiers Media S.A., 7, p. 86. doi: 10.3389/fbioe.2019.00086.

van Doremalen, N. et al. (2020) ‘ChAdOx1 nCoV-19 vaccine prevents SARS-CoV-2 pneumonia in rhesus macaques’, Nature. Nature Research, 586(7830), pp. 578–582. doi: 10.1038/s41586-020- 2608-y.

EDS - DNA Script (2021). Available at: https://dnascript.com/technology/ (Accessed: 28 April 2021).

Eisenstein, M. (2020) ‘Enzymatic DNA synthesis enters new phase’, Nature Biotechnology. NLM (Medline), 38(10), pp. 1113–1115. doi: 10.1038/s41587-020-0695-9.

Ellis, T., Adie, T. and Baldwin, G. S. (2011) ‘DNA assembly for synthetic biology: from parts to pathways and beyond’, Integrative Biology. Royal Society of Chemistry, 3(2), pp. 109–118. doi: 10.1039/c0ib00070a.

Engels, J. W. and Uhlmann, E. (1989) ‘Gene Synthesis [New Synthetic Methods (77)]’, Angewandte Chemie International Edition in English, pp. 716–734. doi: 10.1002/anie.198907161.

Evans, N. G. and Selgelid, M. J. (2015) ‘Biosecurity and Open-Source Biology: The Promise and Peril of Distributed Synthetic Biological Technologies’, Science and Engineering Ethics. Kluwer Academic Publishers, 21(4), pp. 1065–1083. doi: 10.1007/s11948-014-9591-3.

Evonetix and Analog Devices Collaborate on Third-Generation DNA Synthesis Platform (2020). Available at: www.evonetix.com (Accessed: 28 April 2021).

Fischer, M. and Maurer, S. M. (2010) ‘Harmonizing biosecurity oversight for gene synthesis’, Nature Biotechnology. Nature Publishing Group, 28(1), pp. 20–22. doi: 10.1038/nbt0110-20.

Fraser, C. M. and Dando, M. R. (2001) ‘Genomics and future biological weapons: The need for preventive action by the biomedical community’, Nature Genetics. Nature Publishing Group, 29(3), pp. 253–256. doi: 10.1038/ng763.

Frazer, K. A. et al. (2003) ‘Cross-species sequence comparisons: a review of methods and available resources.’, Genome Research. Cold Spring Harbor Laboratory Press, 13(1), pp. 1–12. doi: 10.1101/gr.222003.

Hughes, R. A. and Ellington, A. D. (2017) ‘Synthetic DNA synthesis and assembly: Putting the synthetic in synthetic biology’, Cold Spring Harbor Perspectives in Biology. Cold Spring Harbor Laboratory Press, 9(1), p. a023812. doi: 10.1101/cshperspect.a023812.

Katz, L. et al. (2018) ‘Synthetic biology advances and applications in the biotechnology industry: a perspective’, Journal of Industrial Microbiology and Biotechnology. Springer Verlag, 45(7), pp. 449– 461. doi: 10.1007/s10295-018-2056-y.

Kemp, L. et al. (2021) ‘80 questions for UK biological security’, PLoS ONE. Public Library of Science, 16(1 January). doi: 10.1371/journal.pone.0241190.

Khan, S. et al. (2016) ‘Role of recombinant DNA technology to improve life’, International Journal of Genomics. Hindawi Publishing Corporation, 2016, pp. 1–14. doi: 10.1155/2016/2405954.

Kirk, D. (2019) Building DNA on a chip: a novel approach to gene synthesis.

Kosuri, S. and Church, G. M. (2014) ‘Large-scale de novo DNA synthesis: Technologies and applications’, Nature Methods. Nature Publishing Group, 11(5), pp. 499–507. doi: 10.1038/nmeth.2918.

Kunjapur, A. M., Pfingstag, P. and Thompson, N. C. (2018) ‘Gene synthesis allows biologists to source genes from farther away in the tree of life’, Nature Communications. Nature Publishing Group, 9(1), pp. 1–11. doi: 10.1038/s41467-018-06798-7.

Leitenberg, M. (2001) ‘Biological Weapons in the Twentieth Century: A Review and Analysis’, Critical Reviews in Microbiology. Milton Leitenberg, 27(4), pp. 267–320. doi: 10.1080/20014091096774.

Leitenberg, M. (2003) ‘Distinguishing Offensive from Defensive Biological Weapons Research’, Critical Reviews in Microbiology. Milton Leitenberg, 29(3), pp. 223–257. doi: 10.1080/713610450.

Motea, E. A. and Berdis, A. J. (2010) ‘Terminal deoxynucleotidyl transferase: The story of a misguided DNA polymerase’, Biochimica et Biophysica Acta - Proteins and Proteomics. NIH Public Access, 1804(5), pp. 1151–1166. doi: 10.1016/j.bbapap.2009.06.030.

Noyce, R. S., Lederman, S. and Evans, D. H. (2018) ‘Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments’, PLOS ONE. Edited by V. Thiel. Public Library of Science, 13(1), p. e0188453. doi: 10.1371/journal.pone.0188453.

Palluk, S. et al. (2018) ‘De novo DNA synthesis using polymerasenucleotide conjugates’, Nature Biotechnology. Nature Publishing Group, 36(7), pp. 645–650. doi: 10.1038/nbt.4173.

Pearson, G. S. (2000) Scientific and Technical Implications of the Implementation of the BTWC Protocol - Report on the NATO Advanced Research Workshop, Warsaw, Poland: 2-4 November 2000. Available at: http://hdl.handle.net/10454/777 (Accessed: 28 April 2021).

Perkel, J. M. (2019) ‘The race for enzymatic DNA synthesis heats up’, Nature. NLM (Medline), 566(7745), p. 565. doi: 10.1038/d41586-019-00682-0.

Pfluke, C. A. (2019) An Examination of the Potential Threat of a State- Sponsored Biological Attack Against the United States : A Study of Policy Implications. Missouri State University. Available at: https://bearworks.missouristate.edu/theses/3342 (Accessed: 28 April 2021).

Reding, D. F. and Eaton, J. (2020) Science & Technology Trends 2020 - 2040 - Exploring the S&T Edge (NATO Science & Technology Organisation). Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf (Accessed: 28 April 2021).

Roffey, R. et al. (2002) ‘Biological weapons and bioterrorism preparedness: Importance of publichealth awareness and international cooperation’, Clinical Microbiology and Infection. Blackwell Publishing Ltd., 8(8), pp. 522–528. doi: 10.1046/j.1469-0691.2002.00497.x.

Senior, M. (2020) ‘Europe’s biotech renaissance’, Nature Biotechnology. Nature Research, 38(4), pp. 408–415. doi: 10.1038/s41587-020-0483-6.

Shears, J. (2019) ‘Is there a role for synthetic biology in addressing the transition to a new low-carbon energy system?’, Microbial Biotechnology. John Wiley and Sons Ltd, 12(5), pp. 824–827. doi: 10.1111/1751-7915.13462.

Singh, R. (2011) ‘Facts, growth, and opportunities in industrial biotechnology’, Organic Process Research and Development. American Chemical Society, 15(1), pp. 175–179. doi: 10.1021/op100312a.

Tang, W. L. and Zhao, H. (2009) ‘Industrial biotechnology: Tools and applications’, Biotechnology Journal, 4(12), pp. 1725–1739. doi: 10.1002/biot.200900127.

Teixeira da Silva, J. A. . and Dobránszki, J. (2015) ‘Potential Dangers with Open Access Data Files in the Expanding Open Data Movement’, Publishing Research Quarterly. Springer New York LLC, 31(4), pp. 298–305. doi: 10.1007/s12109-015-9420-9.

Tucker, J. B. (2010) ‘Double-Edged DNA: Preventing the Misuse of Gene Synthesis | Issues in Science and Technology’, Issues in Science and Technology, 26(3), pp. 23–32. Available at: https://issues.org/tucker-2/ (Accessed: 26 April 2021).

Wang, F. and Zhang, W. (2019) ‘Synthetic biology: Recent progress, biosafety and biosecurity concerns, and possible solutions’, Journal of Biosafety and Biosecurity. Elsevier BV, 1(1), pp. 22–30. doi: 10.1016/j.jobb.2018.12.003.

Wolf, Y. I. et al. (2018) ‘Origins and evolution of the global RNA virome’, mBio. American Society for Microbiology, 9(6), pp. 1–31. doi: 10.1128/mBio.02329-18.

Essay Title: Societal Reactions of Emerging Technology

Author: Khadijah Akuji

Institute: Thornhill Community Academy

Abstract

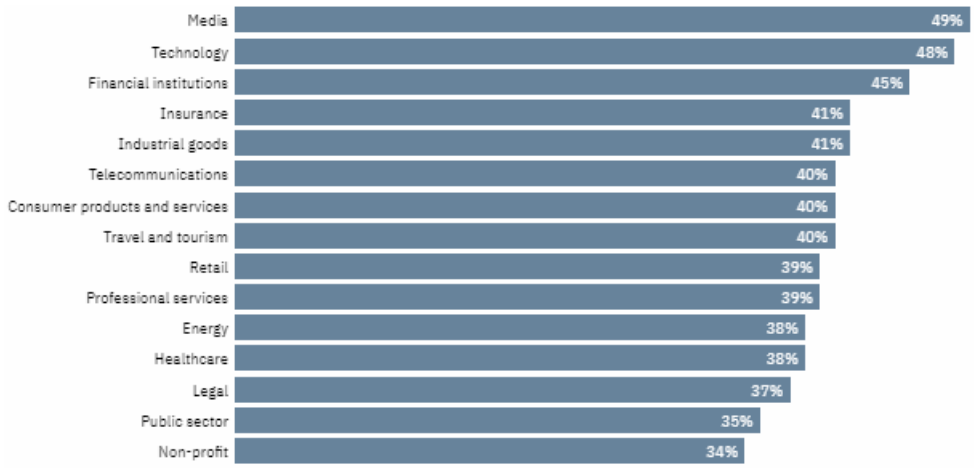
When technology is introduced to the public, it is up to societal reactions that can cause such technologies to prosper. People's reactions to technology are an important resource for researchers and companies hoping to implement them into everyday life. By looking into how the public are affected by introducing and implementing technology, one can learn the ethical and moral, and legal implications it can pose on an average person. This paper focuses on reactions towards automation, AI development, as well as a current use of emerging technology, the NHS' Test and Trace programme.

Introduction

The vast and ever-evolving technology of communication and exploration has had a world-changing effect, especially in maintaining and developing new opportunities for defence and security systems to advance. Technology, as one would define in the present, was first designed by physicist John Atanasoff, and would use binary numbers. From then on, computer technology would evolve at a rapid pace, and create progressively smarter machines which would then be used for individual purposes, to counter their inaccurate counterparts, humans. Emerging technology, while may present opportunities to become a more technologically and data-accurate use for defence and security, may hold bias and unfavourable odds for the civilians that these machines are built to protect. This essay will discuss emerging technology that may be more prevalent in the future and show the social bias these computers hold from when they are in use.

Robots and automation

As technology advances, cheaper, more capable, and more flexible pieces of tech are accelerating the growth of fully automated production facilities. In a Philips plant producing electric razors in the Netherlands, robots outnumber the nine production workers by more than 14 to 1. This wave of automations is said to be driven by the idea of freeing human workers from dirty, dull, or dangerous jobs; improve quality by eliminating human errors; and cut manufacturing costs by replacing expensive people with increasingly cheaper machines. And with over a third of British workers thinking about the risk of their job being automated over the past year, overall



societal reactions are that automation is perceived to prose the biggest threat in their personal finances, and the lack of time to reskill so they can apply for tech roles.

Automation anxiety is not a new, as it occurred during the Great Depression of the 1930s, and the Great Recession of 2007 -2009, when the labour market deteriorated and concerns of machines replacing humans became more worrying. In the present, such automation fears have also collided with the economic uncertainty caused by the pandemic. These concerns are particularly prevalent among jobs in the legal, insurance, media, and financial institutions. While there are many that emphasise their worries about having their jobs taken away, to reduce worries about having robots 'steal away' jobs, efforts should be placed in protecting the people, rather than the jobs.

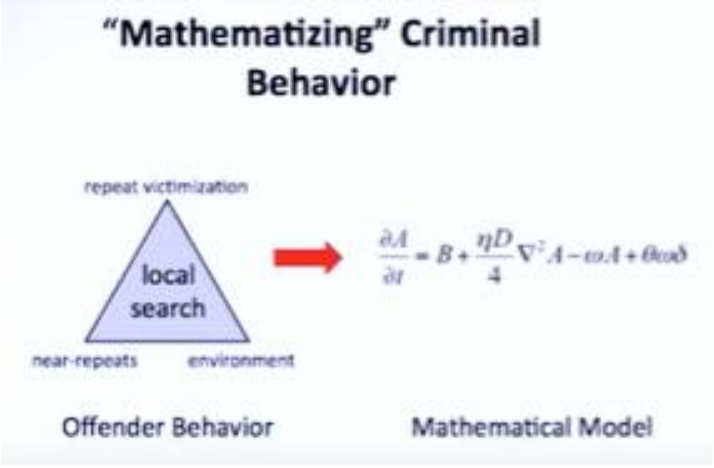
In this instance, societal reactions are based on how companies may choose to manage emerging technology being used for automation and deciding on how to deal with employees whose jobs are in jeopardy of being automated. With ever-evolving technology like robotics, reducing anxiety, especially in financially tight situations such as the COVID-19 pandemic, is crucial for the public to positively view automation, instead of fearing it.

Artificial Intelligence

One of the most well-known breakthroughs of technology to bring data analytics is Artificial Intelligence (AI), which is said to be significant in many fields, due to its ability to enable machine learning like deep learning, which can then be used to perform predictive analytics. The potential of AI is said to emerge in many different critical fields such as cyber defence, risk management, pattern recognition, cyber situation awareness and data correlation to name a few. A main advantage, one may say, is that by using objective data that AI may retrieve and neatly showcase, it removes cognitive bias which can obscure real statistics, and produces results that do not hold any preference or inclination that results may show if a person carried it out. In theory, AI seems to be the perfect solution. This inclines one to believe that AI can produce perfectly factual representations of the areas being monitored and managed, however as one can see by even searching for a modern building on Google Earth, AI is not objective as it seems. While it may seem harmless in this situation (looking for buildings), when substantial decisions and policies are made, like sending police controls, AI is not as perfect as it may seem.

In present day, and more often in the future, many penal systems are beginning to use modelling from these AI programs to answer questions such as which neighbourhoods/areas are to be closely under surveillance, or which prisoners get parole. This is due to the common belief that these models made by computers, are neutral, unlike the opinions of judges or police forces. A common use is plugging in areas where crime is most common, and the program outputs a list of areas to patrol; on surface, it seems to be the logical solution. However, the problem with this method, is that they only output good data if good data is inputted in the first place. For example, in the U.S.A, policing models are built on the question 'where do most crimes occur' and is used to theoretically stop the biggest and worst crimes from happening. However, many these crimes being inputted, are 'nuisance crimes' which are non-violent crimes (vagrancy, panhandling, small-time drug use), and such crimes are more prevalent in poorer areas. Therefore, the map that the program outputs, is just a highlight of these poorer areas.

Mathematician Cathy O'Neil describes in her book 'Weapons of Math Destruction':



"Reading, [Pennsylvania] police chief William Heim had to figure out how to get the same or better policing out of a smaller force. So, in 2013, he invested in crime prediction software… The program processed historical crime data and calculated, hour by hour where crimes were most likely to occur. If they spent more time patrolling these squares, there was a good chance they would discourage crime. And sure enough, a year later, burglaries were down by 23%... [But] this creates a pernicious feedback loop. The policing itself spawns new data, which justifies more policing [in that area]… in our largely segregated cities, geography is a highly effective proxy for race… PredPol, even with the best of intentions, empowers police departments to zero in on the poor, stopping more of them, arresting a portion of those, and sending a subgroup to prison. And the police chiefs, in many cases… think that they're taking the only sensible route to combatting crime. And now they have cutting-edge technology reinforcing their position there, while adding 'science' to the process. The result is that we criminalise poverty, believing all the while our tools are not only scientific, but fair."

AI is an extraordinary piece of technology that is currently being used in the present and will improve in the future. But AI is just a smart algorithm; while it may be able to deep learn in a method more efficient to its human counterparts, it still lacks the rationality a human does, which allows us to use the data it collects to create policies that are benefitting the wider public. By simply relying on pieces of technology, just because it is 'objective', it only pushes forward a more harmful narrative of which are backed up by the data the program has been asked to search for.

Pandemic

With the ongoing COVID-19 pandemic showing responses of many governments across the world implementing different policies such as lockdown polices, different technology was used to create a system in where individuals could track COVID-19 cases around them, and on the occasion, they find themselves testing positive, they could trace all the places they have been to allow others to self-isolate to reduce the spread of the virus. The NHS Test and Trace service was to have a large budget, to avoid a second national lockdown, however failed to deliver its central promise. This may have to be a result of societal reactions, rather than the program itself.

Contract tracing was supposed to be a way to allow the government to track outbreaks and the spread if the virus if needed. Nonetheless, not everyone was pleased about the idea of revealing personal information like their location, or daily journey to strangers, and some approached this idea with great scepticism.

With many reports of restaurant staff using data from contact tracing being used to harass female customers, and numbers of restaurant goers complaining about having their contact details being seen by other customers, it is easy to see the scepticism individuals have when thinking about using the online facility. There have also been cases of people receiving scam track-and-trace text messages, which only further proves why individuals choose not to use this piece of technology. Part of this problem is the already negative view of highly publicised

privacy violations (such as the Facebook Cambridge Analytica data scandal), where may believe that abusing people's personal information without their permission is a widespread problem across many industries.

Negative bias towards technology that is supposed to be a tool for control the spread of the bias just further push along the digital divide, due to misuse causing fear in such people. One may decide not to use the application, because of the many articles showing harassment after retrieving personal information from contact tracing. Rejecting a method that the NHS spent a large budget on gives an idea of how the public may react to technology being used to monitor a future pandemic (and how the scheme ultimately failed). For contact tracing to work as efficiently as expected, the public need to trust that the establishments that hold their data, will look after it correctly. It is all dependent on how the people the scheme was built for if they will use or ignore a future upgrade towards contact tracing.

Conclusion

Societal reactions towards emerging technology are crucial, as to implement such ideas, the people it is supposed to be benefitting must be on the same page. Automation, AI and government applications like Test and Trace are just examples of many instances of emerging technologies, and the future will only develop more with the rapid evolution of technology the present day lives in. It is important to educate oneself about such technologies, as it reduces fear due to misinformation. On the other hand, it is equally as important for governments to reduce understandable fear and anxiety towards new technology, as only then can technology properly thrive.

References

Gregersen, E. G. (n.d.). History of Technology Timeline. Encyclopaedia Britannica. Retrieved July 15, 2021, from https://www.britannica.com/story/history-of-technology-timeline

Sanchez, S. L. S. (n.d.). Artificial Intelligence (AI) enabled cyber defence. Eda Europa Eu. Retrieved July 15, 2021, from https://eda.europa.eu/webzine/issue14/cover-story/artificial-intelligence-(ai)-enabled-cyber-defence

Harris, J. H. (2012, May 1). A Dismal and Dangerous Occupation. Orca Cardiff. https://orca.cardiff.ac.uk/41250/1/2012harrisjphd.pdf

O'Neil, C. (2017). Weapons of math destruction. Penguin Books.

Dane, E., & Rockmann, K.W. 2021. Listen up! Revitalizing our writing to stir our readers and supercharge our thinking. Academy of Management Discoveries, 7(2): 1-7.

J Panovska-Griffiths, L Grieco, E van Leeuwen… - Journal of theoretical …, 2019 – Elsevier

CA Moser, P Yared - 2020 - nber.org

Wise, J. W. (2021, March 10). Covid-19: NHS Test and Trace made no difference to the pandemic, says report. Bmj.Com. https://www.bmj.com/content/372/bmj.n663.abstract

Waseem, D., & Chen, J. (2020, August 10). Contact tracing: why some people are giving false contact details to bars and restaurants. The Conversation. https://theconversation.com/contact-tracing-why-some-people-are-giving-false-contact-details-to-bars-and-restaurants-143390

Kaldis, Byron . "Converging Technologies". Sage Encyclopedia of Nanotechnology and Society, Thousand Oaks: CA, Sage, Law and policy

Branscomb, L. M. . Empowering technology: Implementing a U.S. strategy. Cambridge, Mass: MIT Press.

Raysman, R., & Raysman, R. . Emerging technologies and the law: Forms and analysis. Commercial law intellectual property series. New York, N.Y.: Law Journal Press.

Tilley, J. (2020, October 20). Automation, robotics, and the factory of the future. McKinsey & Company. https://www.mckinsey.com/business-functions/operations/our-insights/automation-robotics-and-the-factory-of-the-future

N. (2021, May 4). Covid-19 has exacerbated automation anxiety but fear of machines is nothing new. Tech Monitor. https://techmonitor.ai/technology/ai-and-automation/covid-19-and-automation-anxiety


[dstl] The Science Inside
Discover More