INVESTMENT RESEARCH

Crime and no Punishment?

Dealing with the New Cyber World

October 2022

Sir David Omand

in conversation with

Sandy Nairn

Executive Director of the Global Opportunities Trust plc

Sir David Omand

Sir David Omand GCB is Visiting Professor in the Department of War Studies, King's College London. His posts in British government service included UK Security and Intelligence Coordinator in the Cabinet Office, Permanent Secretary of the Home Office, Director of the Government Communications Headquarters (GCHQ), and Deputy Under-Secretary of State for Policy in the Ministry of Defence. He served for seven years as a member of the Joint Intelligence Committee (JIC). He is a member of the Senior Advisory Board of Paladin Capital and until 2021 he was the Senior Independent Director of Babcock International Group plc. A Scot, he was born in Glasgow and educated at the Glasgow Academy and Corpus Christi College Cambridge where he is an honorary Fellow. He was awarded an honorary doctorate by Glasgow University in 2019. He has published three books, *Securing the State* (London: Hurst 2010) and (with Prof Mark Phythian) *Principled Spying: the Ethics of Secret Intelligence* (Oxford 2018). His latest book *How Spies Think: 10 Lessons from Intelligence* is now published in paperback by Penguin (July 2021). He is currently writing a book for Penguin Viking on *Crises and how to Survive Them*.

Introduction

It is rare to get the chance to converse with someone who has been directly involved at the coal face of national security with such a breadth of exposure. Sir David not only had a remarkable career in government and the security services; but has retained an interest and engagement not least in the publication of a number of books and articles in related areas. These include Principled Spying: 'The Ethics of Secret Intelligence', 'Securing the State' and most recently 'How Spies Think: Ten Lessons in Intelligence'. This last book simply should be required reading for any investment analyst wishing to understand and avoid the pitfalls of misinterpreting information and the dangers of personal bias.

There is little doubt that cyber-crime has been on a sharply rising trend as criminals become ever more sophisticated and the number of connected devices expands exponentially. Worse still, the emergence of crypto currencies no doubt also assists in the execution of ransomware. If this were not bad enough it has been accompanied by state support in certain jurisdictions. The involvement of the state has extended into all areas of public life with cyber terrorism and misinformation/malinformation now simply a fact of life.

Such is the pervasive nature of the threats it is critical to make sure we have a better understanding of the current environment and how it might evolve. In this we will be better able to calibrate the risks and incorporate them into our analysis. There are few people globally better qualified to consult than Sir David.

A Dialogue with Sir David Omand

Q. Hostile cyber activity seems to cover a very wide spectrum from what can be described as 'mischief making' by hackers, through to state supported serious criminality and finally direct state aggression. Some malign activity in cyberspace looks like a digital extension of what we were used to experience in the traditional analogue world, but some seems to represent new classes of threat we have not had to face before. Perhaps we could start by running through some of the obvious categories.

A. *I use the acronym 'CESSPIT' to describe the dark side of cyberspace: Crime, Espionage, Sabotage and Subversion Perverting Internet Technology. These are categories as old as history but today they come to threaten us digitally. Take a crime such as fraud. Managers and auditors have always known to look out for fraudulent invoices, for example, but today the criminals may have hacked into the company accounting system and covertly altered stored bank details of suppliers so that large payments intended for them are diverted to accounts set up by the criminals and then laundered through a network of offshore accounts. It is the same sort of crime but produces much greater dividends for the criminals. The digital world has also created new classes of crime such as ransomware, denying a company the use of its equipment and data with the criminals demanding a bitcoin ransom for their release. The same is true for espionage. The traditional spy might manage to purloin a few secret documents. The digital hacker with remote access to the system can copy everything in the archive. Companies can discover they have lost to adversaries on the other side of the world the results of expensive corporate research and product design or their negotiating brief for a big contract. Sabotage is now much easier with digital industrial control systems in manufacturing and in critical infrastructure being accessed remotely and malware inserted allowing sabotage at a time of the attackers choosing. And digital attempts to subvert democratic elections is a reality, with social media seeded with fake accounts and used to spread hostile propaganda and disinformation. So in today's digital world the CESSPIT is a real threat to governments, businesses and citizens.*

Q. Does that mean we should be much more cautious about adopting digital and internet-based solutions in business?

A. *No, on the contrary invest but with eyes open. The internet is a life-changing innovation to be embraced. It is the key to much of our social and economic progress. It is already transforming*

economic life in the global south. Combined with affordable internet capable mobile devices and public key cryptography (that allows secure financial transactions on-line) it is a central part of the digital revolution we are living through. It came into its own during the Covid-19 pandemic enabling people to stay in touch with loved ones and crucially enabling business life to continue through remote working and on-line purchasing. To the point where we are now wholly dependent on having internet connectivity to keep the economy going. The problem is that digital adoption got ahead of taking sensible security measures. The Internet of Things is an example with a competitive market initially flooded with internet-connected appliances and gadgets (even children's toys) without cybersecurity. That was a market failure, now fixed by import regulations that require appropriate security. But not before some child abusers were found to have hacked into the cameras of baby monitors

Q. Are companies that keep data about their customers at especial risk from hackers?

A. *Yes, and the financial penalties if caught out having been negligent over the security of customers payment details could put you out of business. I see digitisation as a fundamental transformation of the way we live. Every kind of information about the world and us can now be expressed in strings of numbers: speech and sound, pictures and video, our location and movements, our DNA, and our browsing and purchasing history on the web along with bank and passport details, vehicle and driving licences and much more. Expressed as numbers the information can be easily stored, moved, shared and recovered, but also easily searched and mined – and manipulated as we see with so-called deep fake videos of celebrities apparently saying and doing things they never did. Every internet-connectable device has an IP address, not just our phones but today including traffic lights in smart cities, central heating and home security systems as well as digital watches and health monitors. The pervasiveness of the internet is such that there will soon be over 28 billion such internet connected devices. It is a tool with huge potential for human development, but it also brings with it the capacity to be used for a range of less appetising ends. A non-exhaustive list includes all those CESSPIT threats I mentioned at the outset, together with increased surveillance. Added to this is the potential power of those that control access to key inputs to internet device production (such as rare earth minerals) or have (like Taiwan) dominance in advanced microchip manufacture.*

Q. It has been said that the internet abolishes the constraints of both time and space. This seems obvious in areas such as tax, where corporates can relocate intangible assets to exploit international tax differences and minimise their effective tax charge. Criminals and dictators alike can launder dirty money digitally making it hard to trace where it ends up. Perhaps you could expand on the difficulties these developments pose for security and law enforcement.

A. *Financial transactions take place electronically at just short of the speed of light. A careless click on a dodgy email can instantly take you to a website controlled by the attackers from where malware immediately infects your whole system. The attackers may well then spend months unknown to you exploring the government or company network identifying the most valuable or damaging material to steal. The attacker could be in the next block or on the other side of the planet, it makes no difference to your vulnerability. So unsurprisingly, for example, serious cybercriminals base themselves in jurisdictions where there have nothing to fear from local law enforcement and there are no extradition agreements with Western countries. The operating model of such criminal groups seems clear. They are tolerated, even encouraged, to fund themselves by conducting criminality against us in the West in return for being available when requested to conduct espionage or sabotage operations against Western governments and companies. In the case of North Korea, the criminals are the state, seeking to steal foreign exchange such as the attempted cyber heist of over $900m from the Bank of Bangladesh via the interbank payments system (discovered just in time but not before almost $100m went missing). The solution can only come with more formal and informal co-operation between national law enforcement and cyber security agencies and companies, especially in the finance sector. And in providing greater transparency to crack down on laundering of the proceeds of crime, which has proven difficult given the competitive dynamics.*

Q. **There has always been tension between 'self-regulation' and the use of the law to enforce standards and the potential for political interference. One element of the US legal framework which has been credited with assisting the growth of the internet is Section 230 of the Communications Decency Act. This provides that internet providers are not deemed publishers and hence not responsible for content but does allow content moderation where such content is thought: *"obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."* Is the existing UK legal framework fit for purpose and should providers carry a legal obligation akin to 'publishers'?**

A. *The existing framework is certainly deficient. Internet providers are not publishers but neither are they just operators of the equivalent of a mail delivery service. A new approach is needed. The UK Parliament is considering the Online Safety Bill that marks a new departure in trying to hold tech giants to account. The intention is to protect children from harmful content such as pornography and limit people's exposure to illegal content, while protecting freedom of speech. It will require social media platforms, search engines and other apps and websites allowing people to post their own content to have stated terms and conditions that protect children and to have the ability to enforce those conditions. From on-line stalking to grooming through to the proliferation of child pornography there are many areas of concern where the internet companies themselves will have to invest so that the technology itself can serve to clean up social media. Under the UK proposals*

the regulator Ofcom would have the power to fine companies failing to comply up to ten per cent of their annual global turnover, force them to improve their practices and block non-compliant sites. We wait to see whether Parliament is prepared to pass these ambitious provisions and whether the tech giants will fully cooperate.

Q. Are there technology solutions that will help keep the internet safe for children?

A. *The platform companies have set their own terms and conditions, and thus do accept a responsibility to screen out obviously criminal material such as child pornography. Some have developed sophisticated algorithms for that purpose. But even there, problems exist. To screen out the offensive material it has to be accessed (by so-called deep packet inspection) to determine what it is. Such techniques might be ineffective if end to end encryption has been introduced. But such encryption is, according to the UK Information Commissioner, one of the most reliable ways of protecting the data of people who use large messaging platforms. Hence the row between the UK Government and Meta over their threat to encrypt personal messaging channels and the appeal to the platforms to find new technical solutions to manage that risk. Safety Tech, as it is being called, is an interesting and growing area for private capital investment. I am an adviser to Paladin Capital whose cyber funds are taking a lead in finding small companies with innovative ideas for Safety Tech. It is estimated that $1 billion has already been raised in external investment toward Safety Tech to deliver safer online experiences by protecting users from harmful content, contact, and conduct on the internet. Once you move beyond obviously criminal activity the arguments do get more difficult. What would constitute unlawful hate speech for example differs widely across jurisdictions. And in the case of the United States, the freedom of speech provision in the Constitution is liable to trump any public interest argument in removing such messaging, even if false or defamatory. This is a politically contested space.*

Q. In Chapter 10 of your book '*How Spies Think*', you paint a slightly dystopian view of the future as an illustration of how the political process could be subverted. Is the future already here?

A. *I wanted to illustrate through a fictional scenario how currently available techniques could be used in combination to subvert a democratic election. So I postulated a future election campaign in which the leader of the ruling political party is humiliated by a video on social media showing the politician apparently engaging in unusual sexual activity on an overseas trip (of course a deep fake); leading opposition politicians are smeared by accusations of sharing child pornography found on their House of Commons computers (of course planted by a hack into the system); leaked politically embarrassing emails cause internal splits in one party (the result of another hack); faked conspiratorial news items allege secret collusion by MPs with oil and extractive industry executives*

to thwart the green agenda - made worse by a massive oil spill from an oil tanker (whose control systems had been deliberately tampered with); and leaked details appear on social media about nuclear materials movements along with encouragement of violent protesters to create disruption; and so on and on, all boosted by social media bots set up by a hostile state to amplify the sense of disorder.

All these techniques exist although they have not been used together against the UK. But they could be, hence my warning. But I am optimistic that we can protect ourselves – taking steps that I set out in the book – once we all recognise the nature of the risk. The recent BBC1 TV political thriller series The Capture illustrates dramatically how such techniques could also be used by the authorities and end up eroding the very meaning of truth. I hope that has helped educate the public of the dangers the online world can pose.

Q. There is also a growing debate about the propagation of false narratives and the 'echo chamber' effect of chat rooms and on-line discussion exacerbated by the way algorithms work in concentrating 'like-minded' people. Where does the line between freedom of speech, and deliberate falsehood as incitement, get drawn?

A. *Platforms like Facebook are designed to make it easy for like-minded people to find each other and form online communities. Fine if it is for the purpose of joining up devotees of The Office or tapestry-weaving and to encourage others of similar inclination. In the past oddballs with conspiracy theories and a tendency to violence would have been tiny eccentric minorities in their local communities. But today they can connect up all too easily with others across the country and internationally. They can come to believe they represent a powerful political movement and come together to take violent action based on their conspiracy thinking. That has already happened in the United States. But the American experience shows how hard it is to curb such movements (including QAnon) without infringing Constitutional safeguards upholding freedom of speech.*

Q I have seen commentary attributed to you about 'understanding the enemy' and the signal importance of understanding the nature of the threat. How do you gain the necessary intelligence and co-ordination to assess subversive threats correctly whilst avoiding the potential descent into paranoia or a McCarthyite type environment.

A. *The role of intelligence is to improve decision making through greater knowledge, or less ignorance, depending upon how one looks at it. Secret intelligence has at its core the purpose of discovering information that others are trying to hide. Like any form of knowledge, secret intelligence often warns that the situation is more complicated than previously thought, that the motives of an adversary are to be feared and that a situation may be developing in a bad way. But it is better to know than not. There is nothing new in this. What is new is both the volume of*

communications occasioned by the internet, the levels of data storage and the increased ability to hide such communications. The internet model is founded on users giving away information on the one hand, and commercial organisations harvesting this data to generate income on the other. If security agencies are to anticipate potential threats, by definition, they have to have the ability to obtain and collate data on their targets. We need to distinguish here between the synthesis of data which is available to any internet user and that which is in some way protected. Probably few of the general public realize just how comprehensive a profile can be gleaned by interrogating and synthesizing records that are already in the public domain. This is more relevant for personal financial protection than it is for intelligence work where the targets are naturally seeking to hide anything incriminating.

All the developments I have mentioned are affecting the demands for intelligence about those who mean us harm, the autocrats and their hired thugs, the jihadist terrorists and violent far right extremists, hackers, narcotics and people traffickers and other serious organised criminal groups, including child abuse networks. Information is needed about them as individuals: their identities, their location, their movements, their associates, their methods of financing themselves and of course their intentions. To address this the intelligence services must of necessity 'invade privacy'. However, this is not the mass surveillance posited by exaggerated interpretations of the Snowden allegations. There is no group of analysts in the UK agencies conducting persistent observation of the UK population. Digital surveillance is restricted by statute to protect citizens rights. For example, there has to be justification that it is both necessary and proportionate before authorisation is given to a computer to sift through bulk data, for example using Artificial Intelligence algorithms to search for communications from the IP address of a terrorist suspect. Indeed, to not pursue such investigation using modern data tools would be seen as a dereliction of duty. If this machine search uncovered relevant information then the reasonable next step would for the filtered, selected material to be passed – and only that material - to a human analyst. The key clearly lies in the search criteria used and the appropriate privacy related oversight.

Q. Has the internet become a major factor in radicalisation and is there anything that can be done to counter-act the effect.

A. *We saw the use of modern advertising techniques using striking visual imagery by the so-called Islamic State when it was active to embolden supporters in the West and to try to persuade them to travel to join their fight in Syria and Iraq. Now the violent far right is also becoming adept at using social media to attract new followers and to incite violent confrontation with their opponents in the streets. Ideally their material, including barely disguised neo-Nazi and racist imagery, would be detected and removed by the platforms themselves since such content is illegal in the UK. But that often depends upon the tech companies being notified by the public of the offensive material. There is a unit in the Home Office that specialises in doing that, but the*

offenders are quick to repost material elsewhere, so it becomes a deadly game of whack-a-mole. In the extreme case of the worst violent jihadist recruiting material ((including footage of atrocities) we are told that GCHQ deployed their offensive cyber capability (now part of the new National Cyber Force, a joint organisation with the Armed Forces) to disrupt ISIS. Much of the material pushed out by ISIS thankfully therefore ended up in a cyber black hole.

Q. Where is the dividing line between police countering cybercrime and the activities of the intelligence services?

A. *The police have primacy in investigating crime and gathering evidence so that those believed responsible can be brought before a Court. In the case of serious cyber-crime the police lead is with the National Crime Agency, with the City of London police specialising in financial cybercrime and money laundering. They work with the FBI and Interpol, and with Europol although post-Brexit that is not as straightforward as it was. The UK intelligence services work hand in glove with the police. A vital role is played by the National Cyber Security Centre (NCSC) in Victoria, London which is a part of GCHQ, the UK's digital intelligence agency and has full access to GCHQ's expertise in network attack and other relevant digital technology (on the principle of poachers make the best gamekeepers). An important responsibility is the attribution of cyberattacks to criminal groups or state agencies, which usually rests on careful intelligence assessment. And the attack surface, as we would call, it is continually expanding as more and more households use technology to keep in touch with family and to shop online. The habits acquired during covid lockdowns are here to stay. And the rapidly growing Internet of Things brings more and more technology into the home, including internet enabled security systems. The obvious conclusion is that ever closer working on these developing risks is needed between police services and national intelligence agencies, and between all of them and international partners and the industry. These global threats cannot be managed satisfactorily by any nation on its own, even the United States.*

Q. It is anecdotal, but the banks seem to be less willing to absorb losses from customer on-line cyber theft. If so, it is likely that this is driven by the continued increase in criminal activity targeting both in retail and corporate bank customers. It does not appear that the police have the resources or ability to investigate or prevent these increases.

A. If so, that would hardly be surprising given the cost to the banks of the surge in cyber theft. Why would criminals take the risks of a long prison sentence if caught in armed robbery, jewel or art thefts when greater pay-offs are likely from cyber theft, generally regarded as a white collar crime carrying lesser penalties and with a very much lower risk of being caught since the criminal and the victim can be on different continents. Cyber fraud is also a crime where multiple victims can

be targeted simultaneously at scale. Even if only a very small proportion fall victim the net proceeds can still be substantial. Law enforcement is largely organised on a local community basis to help control traditional crime, but it does not work well when victims are spread across many nations and offenders are in jurisdictions where they cannot be investigated.

Q. Does the risk then have to be borne by the consumer?

A. *Consumers have to accept responsibility for acting prudently. Banks have sensibly had to insist on higher standards of cyber security for those using their services such as mandatory two-factor authentication as well as tightening the security of their banking apps and point of sale systems. Increasingly banks may resist claims on the grounds that clients may have been careless with passwords or the physical security of their devices. Companies are now also sensibly being much more careful in choosing sub-contractors who can demonstrate that they are cyber secure. It is now a requirement, for example, for prime contractors bidding for defence contracts to be able to demonstrate to government that their supply chains also take cyber security seriously.*

Q. The financial sector quickly brings in talent where necessary, often reaching into government in the legal and compliance areas. Given the specialist skills is staff retention a serious problem? Is this likely to be an ongoing issue, does it also apply to the intelligence services and what can be done to mitigate it? Is there a case for scholarships similar to those in the armed forces?

A. *There is no question that this is a serious issue for both the police and intelligence services. The education system produces only a limited number of people with the technical skills to become cyber/communications/cybersecurity specialists. The supply is therefore limited, and demand is increasing and bidding up the rewards. To attract the necessary calibre of entrant the public sector needs to be able to offer a pay and conditions package which, if not highly competitive, is at least not at such a discount to make recruitment impossible. There is also a strong case to be made for actively encouraging the national expansion of training places to increase the supply and to put more effort into recruiting into technology women and under-represented groups. GCHQ is, for example, now offering cybersecurity and software apprenticeships where youngsters can work on real-life projects and earn a degree on the way.*

Q. This is somewhat anecdotal, but an old colleague of mine recently retired and decided to do a graduate degree in data analysis at a prestigious UK university. I think the course was almost entirely Asian with a very high Chinese element. Without seeking to impugn any of the students it does feel to be a strange outcome that the UK is training the next generation of scientists for economic and potential strategic

competitors. Is this outweighed by the benefits of experiencing a Western education and culture or does this raise any concerns?

A. *The UK's education system is an important component of our soft power. Some of the brightest foreign students elect to stay for advanced degrees and to conduct leading edge research working with British researchers. That is of national benefit. An example is the Russian born Konstantin Novoselov who won the Nobel Prize for chemistry in 2010 for his discovery, working at Manchester University, of the revolutionary new material graphene. The university sector is one of the UK's remaining global strengths – and it has to be admitted that its financial viability depends upon the higher fees charged to foreign students. All that said, the risk is well recognised that hostile intelligence services try to exploit our openness (as they do that of the United States) and so the authorities keep a careful eye on overseas applications for study relating to sensitive technologies.*

Q. Do you think the general population takes identity theft seriously enough and enough education in respect of the various methods of obtaining information for nefarious purposes? There does seem to be some education at the school level but not a great deal for the vulnerable elderly.

A. *I think most of us work on the basis that this is something that happens to other people, until it unexpectedly does happen to us when it can be a very time-consuming and extremely fraught affair to unravel the misuse of our identity. There are covert global markets on the dark net where criminals offer for sale to other criminals: passports, bank details and other identity credentials stolen from individuals both through hacks of databases and from physical theft by pickpockets. Recent figures that I have seen show a cloned American Express card with the PIN could fetch US$35, while credit card details generally sell for as little as a third of this price. Stolen online banking credentials to accounts with a minimum balance of US$2,000 can go for US$65 on average. I am told Gmail accounts command a relatively high price at an average of US$156 possibly because few holders use two factor sign on so a compromised email account could open up wider opportunities for fraud. We need to increase educational provision in schools on how to live safely online, from all the threats I have mentioned. An initiative with voluntary organisations working with the elderly would be an excellent idea – in the long run, today's digital natives will themselves become elderly so let us hope their skills will persist into old age!*

Q. You have mentioned before the 'weakest' link issue, i.e. corporate (or government) systems may be very well defended but less so on third party suppliers where regular updates can act as a back door entry point.

A. We are in a continual arms race with the criminals and hostile state hackers. The networks of the major defence, technology and pharma corporations were the first private sector targets of the

APTs – the advanced, persistent threat groups we see operating from Russia, China, Iran, North Korea and now an increasing number of other states as hacking techniques become better known. Those companies have spent a lot of money protecting themselves, and have 24/7 monitoring of their networks to detect intrusions or unusual activity on their networks. So then the attack switched to overseas subsidiaries, accountancy, financial advice and law firms that might be expected to have connectivity with the headquarters system. Then such attacks spread to their major contractors in the supply chain. When that became known and guarded against the attacks took a more sinister turn targeting software companies that supply specialist programmes to major companies.

Q. Do you mean like the Russian NotPetya attack on Ukrainian companies?

A. Exactly. That was an attack by Russian GRU hackers on a small Ukrainian software company whose tax preparation programme was widely used in Ukraine. The hackers managed to infect the updates that were routinely supplied to customers with a virus that locked up their machines and data. Unfortunately, the tax software was also installed in the branch offices of many major US and EU companies that did business with Ukraine. They too got hit. Notpetya's rapid propagation and exploitation of flaws within the Windows system created global business damage estimated at in excess of $10bn. The Danish giant logistics company Moller-Maersk almost lost access to its entire shipping records, which would have probably put it out of business. The company was only saved by their office in Ghana which, because of a power cut, happened to be off-line and so their copy of the key operating system was uncorrupted. Companies will not always be so lucky. Some argue that the Russian target was the Ukraine and the virus escaped through reckless programming whilst others see it as a widespread message for the international community to shun doing business in the Ukraine.

Q. Absent draconian restrictions on vendors is there anything that can be done or are these types of attacks now simply a fact of life and are any observations on developments in the aftermath of the attack? How do smaller companies try to address these cyber issues?

A. There are many lessons to be learned from the NotPetya experience, as there are from other major attacks such as the Wannacry virus that badly affected UK healthcare. There is a great deal of solid advice available to small and medium sized enterprises for free on the website of the National Cyber Security Centre. Some lessons are technical, such as all organisations ensuring that the backups routinely made of key system data are kept offline and cannot be corrupted if there is a successful attack on the system (which is what almost brought down Maersk with NotPetya). Some of the lessons are organisational and cultural and for the Chief Executives and Boards to satisfy. If there were a serious cyber attack how would the rescue be organised and what outside support

would be needed? What facilities with the right communications and connectivity would be available? Who would take charge and from where, including informing and reassuring investors, suppliers, sub-contractors and customers? Reputations can be seriously trashed by perceptions of poor handling. Attempts to gloss over the consequences of attacks can lead to heavy penalties. The questions Boards must ask of the executives is show us the plan - and when did you last conduct an exercise to test it for real? I recommend browsing the comprehensive NCSC website where there is a lot of help for smaller organisations, including an 'exercise in a box' they can use.

Q. Perhaps we could pick up on the question of hostile government involvement. It appears that this runs from actions disruptive to commerce, to intellectual property theft through to actions to subvert the democratic process of Western democracies. Obviously there has been much discussion on both the Brexit process and the 2016 Presidential election. Is there anything you can say about these other instances?

A. *Attempts to use fake news to influence democratic elections are a historical phenomenon. For example, shortly before the 1924 British General Election the Daily Mail published a headline article entitled 'Civil War Plot by Socialists: Moscow Order to our Reds'. The Mail claimed sight of a letter from Gregor Zinoviev, the President of the Communist International to the UK representative of Comintern stating that the Labour Party would help 'paralyse the Army and the Navy' as part of their desire to follow the Russian Leninist model. The letter was a forgery by white Russians opposed to Labour Prime Minister, Ramsay MacDonald's policy of recognising the Soviets. MacDonald duly lost the October 1924 election. Whether the Zinoviev letter was the crucial factor is hard to say, but it has entered into Labour Party mythology as a right-wing plot aided by the British Secret Service. Fast forward to our last General Election and the Foreign Secretary's statement that Russian actors 'sought to interfere' in the last UK general election by amplifying an illicitly acquired NHS dossier that was seized upon by Labour during the campaign. That was an example of 'malinformation'; information that is genuine but was never intended to be used in that way. 'Disinformation' on the other hand is known to be false at the time by those spreading the lies. And we will always have cases of misinformation by politicians and the media where their facts turn out to be wrong – and should be corrected on the record when the innocent mistake is discovered*

Q. Is the development of quantum computing the next big arms race given its potential impact on cryptography etc. How distant do you think the threat is and how would you rank the competing nations?

A. *My response starts by posing a question: what do we think would happen if China were the first nation to develop a quantum computer capable of operating at the scale needed to crack the presently unbreakable public key encryption that protects our financial transactions (the SWIFT*

interbank system for example) and all our sensitive commercial, diplomatic and military communications? I hasten add that no such machine yet exists, although there is lab scale proof of concept (as there has been for power generation from nuclear fusion for some years, although no-one has yet managed to scale it up for commercial production). The race is on and many advanced countries including in the US, UK, EU, China and Japan have relevant research projects. It may take many years, but you cannot rule out an unexpected breakthrough, somewhere. Perhaps using as yet undiscovered novel technologies such as using organic materials for computing, It is impossible to know how a quantum computing machine would be exploited and for how long it could remain secret – and whether in the end sharing the secret might not be the safest route given that any advanced nation stands to lose as well as gain from the ability to defeat hard encryption and the global chaos that would likely follow. The policy conclusion I draw from my initial question is that we would be well advised to put even more effort now into devising quantum resistant algorithms for a secure future.

Q. I assume that there is much that the public can never know about in terms of the authorities taking action to prevent in preventing cyber-crime and penetration. Is there anything you can share to shed some light on these efforts?

A. *The tightly sealed-off old world of secret agencies has been replaced by a model open to law enforcement, seen in the acceptance of intelligence-led policing and, for example, in the intelligence colocation of the Security Service regional hubs with the police. The drafters of the intelligence legislation of 1989 and 1994 anticipated these demands by making it a statutory purpose of the secret agencies to act in support of the prevention or detection of serious crime. The Investigative Powers Act 2016 also acknowledges for the first time, and regulates, the use by the intelligence services of another important recent source, network exploitation or hacking, again under warrant and judicial oversight. A good example is Operation Venetic, the UK's largest ever law enforcement operation, led in the UK by the NCA but made possible by digital intelligence exploitation. A covert operation led by the French authorities with allied partners penetrated the servers located in France of the EncroChat mobile phone company that was providing 60,000 criminals worldwide (10,000 in the UK) with end-to-end encrypted messaging. It is a measure of the power of organised crime that such a company could exist openly providing, for an annual fee, stripped down mobiles without voice or any apps that might provide a toehold for law enforcement exploitation. The results in the UK of being able to monitor criminals talking to each other were spectacular, including recovering £54m in cash, 77 firearms, and more than 2 tonnes of Class A and B drugs. On the other hand, the case illustrates just how criminals have been quick to take advantage of end-to-end encryption services.*

Q. The digital intelligence capabilities we have been discussing are certainly powerful. Looking ahead, are you confident that the liberties and rights of the public will be protected?

A. *Security rests on the sensible management of risk in ways that respect our values including our individual rights. Indeed, public security in a democracy depends upon active support for all security and intelligence authorities in a modern form of Robert Peel's principles for policing: the people are the police and the police are the people. There is a delicate balancing act therefore in upholding our fundamental right to national security and civic harmony whilst maintaining justice, freedom of movement and of speech and privacy. We have to seek balance within the basket of human rights and not a trade-off of rights for security. COVID-19 has shown us what a state of national insecurity looks like, with the premature deaths of more people, and more economic and social dislocation, than any hostile terrorist or cyber-attack could have. For a time, confidence in government to take sound decisions in a timely manner was shaken on both sides of the Atlantic. In future, we will need to treat all major potential disruptions, including those arising from climate change, as well as all the malign threats, as important classes of future national security challenge. And draw the lesson from current and recent crises that we must invest to improve our national resilience and thus avoid disaster.*

Investment Implications

The dialogue with Sir David was fascinating, but simultaneously reassuring and disturbing in equal measure. The reassuring elements included examples of just how much the security services do to protect the public both individually and collectively in the form of public services and corporates. The disturbing elements included the scale, geographic dispersion and state support of the whole range of nefarious activities. What was repeatedly emphasised was the need for close cross border co-operation and consultation.

From an investment perspective there are a few obvious conclusions. The first is that all companies are potential candidate for attack either directly or as collateral damage. The Moeller Maersk example is instructive, barring issues in the Ghanian electricity network one of the world's largest shippers could have been brought to its knees. Imagine also the worst case and the turmoil in world trade if container ships the world over were characterised by a lack of knowledge of their contents. For the analyst the task of understanding the extent of company defences is not one where great deal of confidence can be placed on any external analysis. All companies will claim (and probably believe) that they have devoted all the necessary resources to counter any threat. Perhaps he most one can do is infer from any knowledge of the company's operational IT whether this is likely, i.e. if the company is known for persistent IT issues perhaps one should be wary and investigate further as to whether this is an endemic issue and apply an appropriate valuation risk discount.

Secondly, although not directly a cyber issue the reliance on Asia for components was noted. Pre World War I the Clydeside shipyards produced 40% of the world's shipping tonnage. Although not solely down to war time experiences, many countries decided they could no longer take the risk of being so reliant on an external supplier. 100 years later, for shipyards read electronic components and microprocessors. There are number of processor and components where the geography of supply must be making military and intelligence strategists suffer sleepless nights. Some of these components are manufactured by companies where there are direct or indirect links to the State. Witness for example the restrictions placed on Huawei, one of the world's largest suppliers of telecoms equipment over fears that the company's products could contain deliberate security holes to be exploited by the Chinese government. Concerns are not restricted to companies with these links. TSMC has a technological lead which allows it to dominate the global foundry market. For a Western military strategist, the geographic siting must represent a huge risk.. In the increasingly charged environment where regional blocs appear to be forming, it has to be assumed that the US will progressively require on-shoring of strategically important component design and

manufacture to protect against both physical and cyber threats given the geographic security concerns. The West simply cannot afford a denial of access to these vital components of both the military and industrial complexes. Ultimately this means state support to ensure the success of domestic producers. This means a partial reversal of the benefits of product specialisation and globalisation in the interests of national security.

National security extends well beyond the physical location of key production facilities. Sir David specifically pointed to the emergence of safety tech during the discussion. It must be a huge opportunity with long-run secular growth characteristics. The perpetual ingenuity of criminals combined with the exponential growth of connected devices means that we can only be at the early days of this segment of the market. It is a long-time since we thought Norton Anti-Virus was the solution…

There is a clear need to ensure that the developed world produces enough human capital in the correct areas, specifically in ensuring that certain fields of study are prioritised. Forward thinking corporates will not leave this entirely to government and will no doubt set up 'apprenticeship' programmes by sponsoring students through under and postgraduate courses. This might be at least one indicator of future corporate success? Human capital in this area is only going to become more expensive and it is slightly concerning for the West that there appear to be a large imbalance with Asia in developing these critical skill sets. On the other hand, what is a concern for the West is also a future competitive advantage for Asia.

Finally, despite all the concerns over cyber-crime and terrorist cyber activity, it is important to keep this in context. The benefits of the internet and the connected world are still in the early stages. Remaining vigilant on the accompanying threats is not just prudent but necessary to ensure the investment risk:reward balance is properly considered. However, thinking through the risks should not cloud the fact that benefits vastly outweigh these threats. The Darwinian economic world will envelop both those who do not embrace and adopt the technologies, as well as those who do not do so in a safe and secure manner.

October 2022

DR SANDY NAIRN, CFA, FRSE
Executive Director, Global Opportunities Trust plc

About the Author

Sandy Nairn is the manager of the Global Opportunities Trust plc, a self-managed global equity investment trust, and an experienced professional investor and author of three original books about investment. He has won multiple performance awards for the management of global equity portfolios.

Sandy was a founder and CEO of the independent investment boutique Edinburgh Partners in 2003. It was subsequently acquired by Franklin Templeton Investments in 2018, from which time until July 2022 he has been Chairman of the Templeton Global Equity Group. Before founding Edinburgh Partners, he was Chief Investment Officer of Scottish Widows Investment Partnership, from 2000 to 2003, and Executive Vice President and Director of Global Equity Research at Templeton Investment Management, from 1990 to 2000.

In 2001 he published a book entitled *Engines that Move Markets: Technology Investing from Railroads to the Internet and Beyond*. In 2012 he co-authored, with Jonathan Davis, *Templeton's Way With Money* and in 2021 published *The End of the Everything Bubble: Why $75 trillion of investor wealth is in mortal jeopardy*, warning investors about an imminent severe decline in both stock and bond markets.

Sandy Nairn graduated from the University of Strathclyde in 1982 and in 1985 was awarded a PhD in Economics from the University of Strathclyde/Scottish Business School and has been a CFA charterholder since 1992. In 2020 he was elected a Fellow of the Royal Society of Edinburgh.

Important

This material should not be considered as advice or an investment recommendation. The views expressed within are those of the author and no reliance should be placed on the fairness, accuracy, completeness or correctness of the information or opinions contained herein.

About the Author

DR SANDY NAIRN has more than 35 years of experience in fund management and investment research. He is Executive Director of the Global Opportunities Trust (www.globalopportunitiestrust.com) and the author of three critically acclaimed books about the stock market, most recently *The End of The Everything Bubble* (Harriman House 2021).

www.globalopportunitiestrust.com