Cryptography, crime, terror, and surveillance

Mohit Agarwal

March 2022

Modern encryption methods permit a level of privacy in communication that has not before been seen: information that is encrypted cannot be decrypted without the necessary keys, with algorithms such as RSA where security is ensured by the large primes involved and the current intractability of prime factorisation. This allows for communication that is practically guaranteed to be private; a relatively new phenomenon in communications. In the past, this has been seen with the one-time pad (Rijmenants, n.d.) which was cryptographically secure and used by both the KGB and NSA, well beyond the use of the Enigma and Lorentz machines by the Nazis which were both decrypted through cryptanalysis methods during the Second World War. Today, however, secure cryptographic methods are used not only by government backed agencies in preventing or practising espionage, but by individual citizens who are interested in their privacy, security, or are simply using a computer program that happens to encrypt their communications. Naturally, current availability of cryptography potentially allows malicious actors such as criminals or terrorists to use encryption in order to commit crimes or acts of terror. In response to the threats of encryption and communications technology generally, governments have engaged in signals intelligence (Sigint) such as phone line tapping. Modern Sigint initiatives have become rather complex and sophisticated and have grown greatly alongside the popular adoption of information technology. Part of government interest in Sigint is a direct response to perceived threats, such as the PATRIOT Act in the United States which followed the 2001 terrorist attacks with the objective of strengthening national security (H.R.3162, 2001). Later, the FISA Amendments Act of 2008 further increased the powers of law enforcement to access information, such as allowing the Attorney General and Director of National Intelligence to gather information about individuals outside the United States (H.R.3773, 2008). It was, however, the PATRIOT Act and FISA Amendments Act that was the justification for large scale surveillance including the government access of phone calls records of customers of the Verizon network, including calls from the United States to other states as well as calls localised entirely within the United States (Greenwald, 2013; Roberts, 2013; Savage, 2013). State sponsored Sigint programmes such as that in the United States aims to respond to encryption and other technological

developments with the primary interest of overcoming it in order to prevent terror and crime. These measures have, however, had arguably limited effectiveness and have violated the privacy of individuals who are not suspected to be a threat to national security. Responses to encryption will have significant consequences, given the potential importance of the information being communicated and the prevalence of electronic communication methods. Successful Sigint and cryptanalysis by government agencies can respond to modern threats of crime and terror. A failure of responsible governance, however, may not only threaten the privacy of individuals unnecessarily but also fail to respond to the ways in which criminals and terrorists are using encryption, existing thereby only as a tool of authoritarian control.

An argument is often made against allowing widespread use of encryption and generally against widespread effective operations security (OPSEC) in the public sector in the interest of national security and the prevention of terror. With access to communications and usage history, governments can gather significant information on terrorists and use this intelligence against terrorists. It is clear that intelligence and surveillance play a significant role in counterterrorism. The 9/11 terrorist attacks are seen potentially as a phenomenal failure of intelligence as detailed in The 9/11 Commission report (2004). The report explores the fact that there was potentially knowledge to indicate a terrorist attack before September 2001 (chapter 8). The report details institutional failures and also emphasised the difficulty and importance of intelligence in counterterrorism (Byman, 2014). Graham (2016) explores the use of encryption by terrorists which is often cited as a reason for giving governments access to unencrypted Internet communications so that suspicious activity can be flagged and investigated in order to prevent a terror attack or in order to better respond in the case of an attack. Graham describes the extensive use of end-to-end encryption by terrorists in order to avoid interception by the authorities. Due to U.S. usage of intercepted communications to uncover and prevent a number of al-Qaeda plots, the terrorist organisation and other terrorist groups have increasingly used encrypted communications. A significant factor is the use of non-mainstream software in the early use of encryption by terrorists, including a program that built a wrapper around the popular, secure, and open source PGP called *Mujahedeen Secrets* by al-Qaeda. Although now terrorists and criminals use widely available, popular, and user-friendly software such as the Tails operating system or Telegram, terrorist organisations have shown an ability to make use of more obscure and complicated systems, as well as to use publicly available source code in order to construct software for operatives to use.

Although the issue of popular messaging technologies and their support for end-to-end encryption is often discussed, the argument that the introduction of end-to-end encryption by large companies such as Facebook gives an advantage to

criminals (Musotto, 2019; Home Office, 2020) is arguably an invalid one. By preventing the usage of true end-to-end encryption in industry, we will not be able to prevent those attempting to evade the law from doing so, as shown in the case of terrorist organisations who have used more obscure software in the past and also in the case of the abundance of illegal activity that occurs on the so-called 'dark web' in the form of the trade of drugs and child pornography among others (Gulati, 2018). Instead, the limitation of use of encryption on popular software will only decrease the privacy of those uninterested in criminal activity and instead using more popular software without regard for its security features or lack thereof. The information exposed by Edward Snowden in 2013 demonstrates that the US government has processed and collected vast amounts of unencrypted data and possibly continues to do so. In the case of unencrypted communication, the problem remains and preventing end-to-end encryption will simply allow governments to maintain the status quo of being able to intercept and read all communications between their citizens and individuals outside of their jurisdictions. Indeed, should end-to-end encryption continue, perchance, to be opposed by governments both in the West and in countries like China, it will arguably a method of allowing a government to practise surveillance and of perpetuating a surveillance state.

In the GDR (German Democratic Republic, also known as 'East Germany'), in order to conduct surveillance on behalf of the ruling party (Jarausch, 2014), the Stasi (*Ministerium für Staatssicherheit*, or "Ministry for State Security") relied on a sprawling network of informants and agents. In particular, informants – who greatly outnumbered agents (Bruce, 2014) – formed large parts of this network and were deeply integrated into the fabric of society. This contributed to a far more complete surveillance state and an atmosphere of terror amongst the people. Whilst in Nazi Germany there may have been around one Gestapo agent for every 2300 citizens, in the GDR it was closer to one informant or officer for every 63 citizens. Those living in the GDR often had experiences involving investigation by the Stasi and there was clearly an understanding amongst citizens that one had to be wary of an informant or agent listening in (Funder, 2003). In modern Western society, there is a similar collective understanding that governments carry out surveillance on a massive scale on their own citizens. A key distinction today, however, is that this work is not carried out by a vast network of informants, there are no kilometres of paper, and there are no collections of film and photographs (The Federal Archives, n.d.) documenting and aiding the surveillance of the authorities. Instead, the level of surveillance that large, secretive groups of individuals once had to carry out in order to enable a surveillance state can be performed through bureaucracies and technological methods. In modern times, governments can operate with a very limited number of operatives 'on the ground' and instead focus attention on the giant amounts of data they have for processing in order to make the findings

they intend to: be it crime, terrorism, or – as was the case in the Gestapo and Stasi – dissent.

- -

As has occurred with technological developments in the past, legislation will continue to follow developments relating to information technology, such as the General Data Protection Regulation in the European Union which has had significant influence in the technology industry (EUR-Lex, n.d.; Downes, 2018). Yet encryption presents unique challenges to lawmakers. Not only will encryption be difficult to regulate due to its rapid development, but perhaps expressly due to its decentralised nature, where a government cannot prevent the existence of software that enables encryption that is open source and reproducible internationally. Just as media piracy through torrents and access to hidden services over Tor are able to evade regulation, regulation of encryption may prove impossible. An arguably useful tool to the authorities does exist in the hardware and infrastructure that users of the Internet rely on. In the West, a small number of companies (such as Intel, Nvidia, Arm and Apple) design and produce the majority of hardware in a proprietary and closed source manner.

Concerns have already been expressed with regard to the Intel Management Engine (Portnoy, 2017) that exists on modern processors produced by Intel. Arguments have been made that the Intel Management Engine already acts as a backdoor for government agencies (Wallen, 2016), and the potential is clearly there for US government interests in mass data collection and Sigint following 9/11 to lead to the introduction of backdoors in popular technology. We are aware that in the case of the Intel Management Engine a switch for disabling functionality is present for use by US government authorities such as the NSA, demonstrating the level of leverage the US government potentially has over organisations including but not limited to Intel (Claburn, 2017; Cimpanu, 2017). The potential exists for such systems to be built into non-open hardware which most people – even those using open software – use, leaving them open to exploitation from either state or private actors. Furthermore, there is a visible interest in increasing the presence of technologies on the hardware level, including the aforementioned Intel Management Engine, the Trusted Platform Module (Warren, 2021), and recently Microsoft's Pluton (Goodin, 2022) subsystem which will be present on hardware sold in the future. This variety of hardware within a single computer is a rather interesting and potentially worrying development, particularly with the clear level of influence, interest, and competitiveness both the United States (Shah, 2022) and Chinese governments have in their respective national chip manufacturing industries. In light of potential issues with hardware, there have been developments in ‘open

hardware'.

RISC-V is an instruction set for processors from the University of California at Berkeley; as opposed to Arm, Intel, and AMD processors, RISC-V is an open standard for CPU design (Asanović, 2014). This allows for open source CPU implementations, such as those designed at UC Berkeley, as well as those from other parties, such as Alibaba Group (Chen et al, 2020). A significant amount of existing software has been ported to the RISC-V platform and alongside the Alibaba implementation for data centres, the standard has been used by Google for a security module in the 'Pixel 6' smartphone (Kleidermacher, 2021). This attention and interest potentially signals a shift towards increased demand for and utility in open hardware for privacy, security or economic reasons. Another poignant example of open hardware is the laptop created by the manufacturer Framework Computer Inc, which is designed to be more expandable, serviceable and repairable than other laptops available on the market. The company and laptop gained significant media coverage (Lee, 2021; Klosowski, 2021) showing an interest from the public in open hardware. An argument can be made that such projects are for niche interest groups only and that such solutions will never see the commercial success seen by the larger, non-open manufacturers. However, the clear adoption of standards such as RISC-V by large institutions demonstrates quite the opposite: that open hardware will continue to become increasingly prevalent and that currently popular hardware with its susceptibility to surveillance will possibly have a reduced presence in the future.

Movement towards open standards in both hardware and software reveals a problem for law enforcement agencies and counterterrorism forces. The tools of mass surveillance that once enabled investigation into crime or terror such as reading messages and e-mails, listening to calls or tracking location may no longer be effective, thereby potentially preventing such investigation to occur. For governments, this is arguably the result of such heavy surveillance in the first place. It is clear that knowledge such as the 2013 Snowden leaks had an impact on the public and people are thereby more interested in their privacy and preventing surveillance. Around the world, individuals use tools to increase their privacy and anonymity when using the Internet as well as to overcome censorship of information by governments. A major exception to the availability of the free Internet has been China, where the government has unparalleled and unprecedented control over the flow of information over the Internet. This has allowed the filtering of content, prevention from accessing sites, and the blocking of the anonymity network Tor which would allow users to circumvent measures put in place by the government (Economy, 2018; Talbot, 2009; Winter, 2012). Measures in China have enabled the government to tightly control and monitor the flow of information via the Internet; ensuring that citizens can only access that which the ruling party should allow. Whether such draconian measures

could even be implemented in the more democratic West is questionable, but the opportunity clearly exists for governments to undermine the digital privacy of their citizens. Any such measures, however, will face scrutiny from the media and public in Western society and thereby open software such as Tor is used to freely share significant amounts of information away from the observation of law enforcement, allowing illegal activity to occur (Gulati, 2018). The reduced ability for law enforcement to investigate crime will clearly have an impact by allowing criminals to act with additional impunity. In particular, the sharing of child sexual abuse material, trafficking and other such crimes that are enabled by the Internet present reason for concern.

It is, however, clear that the methods available to law enforcement are not all exhausted due to technological change. Social engineering methods; communications traffic analysis such as phone records; metadata analysis from the underlying infrastructure of the Internet, including public blockchains and Internet Service Provider data; and traditional methods, such as searching for contraband goods are all available to law enforcement despite measures used by criminals or terrorists such as encryption. Indeed, one could argue that the limitations on law enforcement investigations due to technology have a limited impact on the efficacy of investigation, as other sources of evidence have been effectively explored when encryption has been used, particularly in the prevention of terror (Graham, 2016). Thus, encryption might only have a limited impact on law enforcement investigations whilst having a serious impact on user privacy. Although encryption can prevent some investigation the compromise is arguably acceptable due to the net benefit encryption offers to society.

The rate of development in unconventional computing methods is increasing rapidly. Effective quantum computing will result in existing popular cryptographic algorithms such as RSA, which is used for communications and digital signatures, no longer being secure (Chen, 2016). Significant research in recent years has shown feasibility in current ideas surrounding quantum computing and promising results in development towards quantum supremacy and the future breakdown of current cryptographic methods. Indeed, both in the US at Google (Gibney, 2019) and in China at a major university (Ball, 2020; Zhong et al, 2020), claims of 'quantum supremacy' have been made, suggesting that quantum computers will soon become powerful enough to start making current encryption methods obsolete. Although this will not be an overnight transformation, changes will be made by those implementing cryptography, both in the open source space and in industry, as well as in government where government agencies must act in order to protect their data. This change will take place naturally and some have begun to consider methods for post-quantum cryptography (Alagic, 2020). Regulatory considerations about post-quantum cryptography are already being made and arguments can be made that regulation

should soon be written that institutes standards and requirements in order to prepare for a future with effective quantum computing (Bruno, 2021). Once more, however, an issue reveals itself with the incongruity between the speed of regulatory change and the progress of technology. Changes will likely be made by open software in order to maintain secure encryption, such as those used by the open source web servers to encrypt Internet traffic, as well as by large corporations such as Microsoft which provides software used by many businesses and individuals. An issue may exist in software that is less popular and legacy software which may not be open to the scrutiny of open software and may lead to vulnerabilities. Furthermore, the usage of post-quantum cryptography by the public and the potential that it may help terrorists and criminals to communicate might not be addressed in any meaningful way. The lack of high level interest, initiative or funding from governments has arguably prompted more independent development in the public sphere: the US National Institute of Standards and Technology (NIST) made a public request for nominations of post-quantum cryptographic algorithms (Chen, 2017), leading to standards that will clearly influence future lawmaking. This adoption of open processes and the open auditing and implementation of future cryptographic standards is most striking when compared with the *Dual_EC_DRBG* algorithm. This algorithm, which contained a vulnerability, was included in NIST standards. The vulnerability allowed the NSA to potentially decrypt Internet traffic such as e-mails. The NSA also allegedly paid the firm RSA Security in order to implement the algorithm with its backdoor in their popular security products (Menn, 2013) and although the NSA denies wrongdoing there was clearly NSA involvement with the company that remains significant in the enterprise security space (Goodin, 2013; Perlroth, 2013).

Individuals around the world have clearly expressed interest in matters of privacy and encryption and open source software allows those with the technical skills to become involved in the development of technology that enables strong encryption and overcomes state surveillance. Measures taken by governments to prevent this development will doubtless be limited unless extreme actions such as those seen in China are taken. Otherwise, development will continue to occur in both free and non-free societies in support of individual freedoms. The assertion of 'Linus' law' that, "given enough eyeballs, all bugs are shallow" creates a serious inability for actors such as governments to engineer backdoors into software as the NSA previously has or to prevent the development of software altogether. On the other hand, the vast majority of the software and hardware used by the general public is proprietary. For many, this will continue to be the norm. Yet, the pressure from increasing popular open source software will continue to mount. The open source messaging platform 'Signal' offers a security oriented product and publishes requests they receive from courts and law enforcement alongside their replies online (Signal, 2021; Farivar, 2016).

Demonstrating their respect for user privacy and that they are unable to release data as they do not collect it is perhaps something that users are finding more appealing. Indeed, when Apple refused to unlock a phone for the FBI following a terrorist attack it gained significant media attention and demonstrated that the defence of users' privacy was a virtue for modern businesses, regardless of the fact that the FBI was able to unlock the phone independently, which was rather overlooked (Cook, 2016; Yadron, 2016). To users today, both those with experience and ability in technology and to the general public, privacy is seemingly becoming a major selling point and a significant factor in the way individuals chose to use technology.

Modern cryptographic algorithms are theoretically secure; the underlying concepts mean that breaking the encryption to intercept a communication is not possible in a reasonable amount of time with current computational limits and is, therefore, due to the nature of the algorithm, secure. This, however, does not consider implementational flaws. Indeed, implementational flaws are the ways in which modern exploits of algorithms such as RSA occur, and methods such as timing attacks and voltage level analysis attacks, as well as memory attacks (Wong, n.d.; Barenghi, 2009; Aldaya, 2019) have the potential to overcome any level of theoretical sophistication that cryptographic algorithms may have, and simply give away information such as keys. In addition to this, there can be implementational issues in hardware, such as the recent Spectre vulnerability which was discovered in 2018; revealing data to an attacker due to flaws in speculative execution which speeds up processing in modern processors. The vulnerability allowed for the attack of cryptographic implementations such as GPG. This is potentially even more concerning given that processor implementations are proprietary. This flaw, which affects practically every modern processor and indicates the potential for vulnerability in computer hardware, could be exploited by any party with sufficient resources. Intel has released multiple patches for Spectre, however, there remain concerns that there is a potential for attacks in modern processors including new processors made after 2018, and therefore potentially a real threat to security (Kocher, 2019).

The discussion of encryption and related technologies has arguably limited impact. State actors such as the NSA will continue to act against individual freedoms and attempt to find or introduce backdoors in technology that is widely used as part of its actions purportedly in the interest of national security. Although public reactions to information such as the 2013 Edward Snowden releases have been very strong, they have not had significant affects on legislature, the funding received by the NSA, and quite possibly the level of surveillance carried out by the NSA. Thus, discussions in public or private spheres are unlikely to influence decisions made inside already secretive agencies where governments are ready to accept that sacrifices must be made for the

greater good. Of course, the issue arises when surveillance exists that does not exist simply to protect a nation, but instead mass, indiscriminate surveillance is carried out on citizens not suspected of any criminal or terrorist activity such as the Tempora programme in the United Kingdom (MacAskill, 2013), however governments nonetheless prove willing to fund the activities of surveillance agencies and will seemingly continue to do so regardless of public opinion.

- -

The executive summary of the 9/11 Commission Report (2004) describes the September 2001 terrorist attacks as 'a shock, not a surprise'. In a similar light, the release of information relating to mass surveillance and mishandling of data such as the 2013 Edward Snowden releases ought to also be potentially considered a shock, not a surprise, given the level of data that both governments and private organisations have access to and responsibility for. Encryption enables people to trust companies and governments with the handling of communications such as e-mails and enables companies to be able to work with law enforcement without compromising user privacy as encrypted data cannot be read and is therefore useless to authorities. The free market in the West arguably has moved itself towards encrypted standards. Open source initiatives have pioneered free implementations of secure cryptographic standards, allowing any user to use these tools directly in order to send information, such as the popular PGP implementation GPG. Additionally, the open implementation of cryptographic tools enables developers to integrate secure versions of these tools into new programs, allowing for the easy development of programs that allow encrypted communications. The demand for cryptography in less popular open source applications is arguably expected, yet there is nonetheless widespread adoption in more popular software and proprietary software. Companies such as Facebook have pushed for end-to-end encryption in their products and the software industry at large has adopted encrypted standards such as HTTPS. The largest source of resistance to encryption is government intervention. Government positions around the world which are opposed to encryption seemingly have double standards. Just as the Enigma and Lorentz machines were critical to the Nazi war effort in order to conduct critical communications and the breaking of those ciphers were critical to the Allies, encryption remains critical to government communications and state sponsored espionage. Governments maintain up to date cryptographic systems in order to keep their own secure, yet fight hard against encryption in the name of national security. In some ways this is a valid argument: the availability of cryptography arguably lowers the barrier to entry for terror or crime and reduces the ability law enforcement has to deal with it. Nonetheless, it seems that reducing the availability of encryption to the public would not decrease the opportunity for criminals or terrorists to do harm.

Often we see two possible future realities: one with a perfect surveillance state and police state ruled by fear and one with ultimate privacy and total encryption. Both are open to significant abuse with those acting on behalf of the ruling state violating the privacy, basic freedoms and rights of the people in the former. In the latter criminals are able to use technology both to hide their activities and enable their crimes without fear of police interference; creating a near anarchic existence. It seems that in the West, representations of the former in dystopian cultural works such as those by George Orwell or Margaret Atwood and journalistic coverage of government surveillance and oppression in China form our view against highly invasive state surveillance. Yet media coverage of criminals and terrorists using technology and encryption, particularly following events of terror; media and government discussing the risks of technology; and the coverage of law enforcement using surveillance tools to stop criminals shape our view of the latter scenario. I feel, however, that this is a fallacious dichotomy that we have collectively created. In the West, it seems that we have come too far for complete surveillance to be effectively implemented, as the tools to overcome such a regime already exist and there is a widespread sentiment of resistance amongst the public and in governments and courts against such invasive measures. Yet, even in a world of widespread encryption, governments and law enforcement would demonstrably still be able to conduct surveillance and investigation at some level. It is clear that in the Internet age, it is no longer as easy to disguise or hide the truth as it once was. Information has been shown extremely powerful in subverting totalitarianism (Nicholson, 2014) and due to the Internet regimes are less and less able to manipulate the truth. I feel that the most interesting developments in the near future will be how the Chinese government and people will react to developments in technology and if the current state of surveillance, censorship and propaganda will prevail as well as developments relating to encryption and surveillance in the developing world wherever information technology has not yet been widely available. In the West it seems that a reasonable understanding is that being able to use encryption and live without fear of ongoing surveillance relies on a people's will to do so and enact such ideas in their own behaviour, even if certain societal risks are accepted alongside that.

Our fear of crime and terror is justified but it seems that crime and terror will find ways of existing regardless of policy that is not excessively draconian. Terrorists are sometimes untrusting of modern technology and prefer simply to meet in person, outside of the reach of surveillance or Sigint. To fight crime and terror, it seems we must turn to their root causes and ensure that ongoing deliberation and logical dialectic on these complex issues shape policy in a manner more informed and logical than simply engaging in such paranoid measures as total mass surveillance or making encryption illegal or difficult to access for the public.

References

Alagic, 2020.

Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone, "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process," *National Institute of Standards and Technology* (July 2020). DOI: 10.6028/NIST.IR.8309.

Aldaya, 2019.

Alejandro Cabrera Aldaya, Cesar Pereida García, Luis Manuel Alvarez, and Billy Bob Brumley, "Cache-Timing Attacks on RSA Key Generation," *IACR Transactions on Cryptographic Hardware and Embedded Systems* **2019:4**, p. 213–242 (2019). DOI: 10.13154/tches.v2019.i4.213-242.

Asanović, 2014.

Krste Asanović and David A. Patterson, "Instruction Sets Should Be Free: The Case For RISC-V," *Electrical Engineering and Computer Sciences*, University of California at Berkeley (Aug 2014).

Ball, 2020.

Philip Ball, "Physicists in China challenge Google's 'quantum advantage'," *Nature* (Dec 2020). https://www.nature.com/articles/d41586-020-03434-7 Accessed 13th January 2022.

Barenghi, 2009.

Alessandro Barenghi, G.M. Bertoni, Emanuele Parrinello, and Gerardo Pelosi, "Low Voltage Fault Attacks on the RSA Cryptosystem," *Conference: Sixth International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2009, Lausanne, Switzerland, 6 September 2009* (September 2009). DOI: 10.1109/FDTC.2009.30.

Bruce, 2014.

Gary Bruce, "Participatory Repression? Reflections on Popular Involvement with the Stasi," *Bulletin of the German Historical Institute*, German Historical Institute Washington DC (2014). https://www.ghi-dc.org/publication/stasi-at-home-and-abroad-domestic-order-and-foreign-intelligence .

Bruno, 2021.

Luigi Bruno and Isabella Spano, "Post-quantum encryption and privacy regulation: Can the law keep pace with technology?" *European Journal of Privacy Law & Technologies*(1) (2021). https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1225 .

Byman, 2014.

Daniel Byman, "The Intelligence War on Terrorism," *Intelligence and*

National Security **29:6**, pp. 837-863 (2014).

Chen, 2016.
Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone, "Report on Post-Quantum Cryptography," *National Institute of Standards and Technology* (April 2016). https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf .

Chen, 2017.
Lily Chen, Dustin Moody, and Yi-Kai Liu, "Post-Quantum Cryptography, Call for Proposals," *National Institute of Standards and Technology Computer Security Resource Center* (2017). https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals Accessed 25 March 2022.

Chen et al, 2020.
Chen Chen et al, "Xuantie-910: A Commercial Multi-Core 12-Stage Pipeline Out-of-Order 64-bit High Performance RISC-V Processor with Vector Extension," *ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)* (2020). DOI: 10.1109/isca45697.2020.00016.

Cimpanu, 2017.
Catalin Cimpanu, "Researchers Find a Way to Disable Much-Hated Intel ME Component Courtesy of the NSA," *BleepingComputer* (Aug 2017). https://www.bleepingcomputer.com/news/hardware/researchers-find-a-way-to-disable-much-hated-intel-me-component-courtesy-of-the-nsa/ Accessed 6th February 2022.

Claburn, 2017.
Thomas Claburn, "Intel ME controller chip has secret kill switch," *The Register* (Aug 2017). Accessed online on 6th February 2022.

Cook, 2016.
Tim Cook (February 2016). https://www.apple.com/customer-letter/ Accessed 25 March 2022.

Downes, 2018.
Larry Downes, "GDPR and the End of the Internet's Grand Bargain," *Harvard Business Review* (April 2018). https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain Accessed 25 March 2022.

Economy, 2018.
Elizabeth C. Economy, "The great firewall of China: Xi Jinping's internet shutdown," *The Guardian* (2018).

EUR-Lex, n.d..
EUR-Lex, *Procedure 2012/0011/COD* (n.d.). https://eur-lex.europa.eu/procedure/EN/201286 Accessed 25 March 2022.

Farivar, 2016.
Cyrus Farivar, "FBI demands Signal user data, but there's not much to hand over," *Ars Technica* (October 2016). Accessed online on 26 March 2022.

Funder, 2003.
Anna Funder, "Stasiland" (ISBN 9781783787340), Granta Books (2003).

Gibney, 2019.
Elizabeth Gibney, "Hello quantum world! Google publishes landmark quantum supremacy claim," *Nature* (Oct 2019). https://www.nature.com/articles/d41586-019-03213-z Accessed 13th January 2022.

Goodin, 2013.
Dan Goodin, "RSA issues non-denying denial of NSA deal to favor flawed crypto code," *Ars Technica* (Dec 2013). https://arstechnica.com/information-technology/2013/12/rsa-issues-non-denying-denial-of-nsa-deal-to-favor-flawed-crypto-code/ Accessed 5 March 2022.

Goodin, 2022.
Dan Goodin, "Coming to a laptop near you: A new type of security chip from Microsoft," *Ars Technica* (January 2022). Accessed online 25 March 2022.

Graham, 2016.
Robert Graham, "How Terrorists Use Encryption," *CTC Sentinel* **Volume 9, Issue 6** (June 2016). https://ctc.usma.edu/how-terrorists-use-encryption/ Accessed 22 January 2022.

Greenwald, 2013.
Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian* (June 2013). Accessed online on 17th February 2022.

Gulati, 2018.
Saksham Gulati, Shilpi Sharma, and Garima Agarwal, "The Hidden Truth Anonymity in Cyberspace: Deep Web," *Advances in Intelligent Systems and Computing* **673**, p. 719–730 (2018). DOI: 10.1007/978-981-10-7245-1_70.

Home Office, 2020.
Home Office, *International statement: End-to-end encryption and public safety* (Oct 2020). https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety Accessed 29 January 2021.

H.R.3162, 2001.
H.R.3162, *107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001* (2001).

H.R.3773, 2008.
H.R.3773, *110th Congress (2007-2008): FISA Amendments Act of 2008* (2008).

Jarausch, 2014.
Konrad Jarausch, "Between Myth and Reality: The Stasi Legacy in German History," *Bulletin of the German Historical Institute,* German Historical Institute Washington DC (2014). https://www.ghi-dc.org/publication/stasi-at-home-and-abroad-domestic-order-and-foreign-intelligence .

Kleidermacher, 2021.
Dave Kleidermacher, Jesse Seed, Brandon Barbello, and Stephan Somogyi, "Pixel 6: Setting a new standard for mobile security," *Google Security Blog* (October 2021). https://security.googleblog.com/2021/10/pixel-6-setting-new-standard-for-mobile.html Accessed 25 March 2022.

Klosowski, 2021.
Thorin Klosowski, "A Notebook You Can Repair," *New York Times Wirecutter* (October 2021).
https://www.nytimes.com/wirecutter/reviews/framework-laptop/ Accessed 25 March 2022.

Kocher, 2019.
Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom, *Spectre Attacks: Exploiting Speculative Execution* (2019). DOI: 10.1109/SP.2019.00002.

Lee, 2021.
Dave Lee, "Why Big Tech should embrace the 'right to repair' revolution," *Financial Times* (August 2021). Accessed online on 25 March 2022.

MacAskill, 2013.
Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian* (June 2013). Accessed online on 2 April 2022.

Menn, 2013.
Joseph Menn, "Exclusive: Secret contract tied NSA and security industry pioneer," *Reuters* (Dec 2013). https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220 Accessed 5 March 2022.

Musotto, 2019.
Roberto Musotto and David S. Wall, " Facebook's push for end-to-end encryption is good news for user privacy, as well as terrorists and paedophiles," *The Conversation* (December 2019). https://theconversation.com/facebooks-push-for-end-to-end-encryption-is-good-news-for-user-privacy-as-well-as-terrorists-and-paedophiles-128782 Accessed 22 January 2022.

National Commission on Terrorist Attacks Upon the United States, 2004.
National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (9/11 Report)* (July 2004).

Nicholson, 2014.
Esme Nicholson, "The Cold War Broadcast That Gave East German Dissidents A Voice," *NPR* (November 2014). Accessed online on 2 April 2022.

Perlroth, 2013.
Nicole Perlroth, "Government Announces Steps to Restore Confidence on Encryption Standards," *The New York Times* (September 2013). https://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/ Accessed 5 March 2022.

Portnoy, 2017.
Erica Portnoy and Peter Eckersley, "Intel's Management Engine is a security hazard, and users need a way to disable it," *Electronic Frontier Foundation* (May 2017). https://www.eff.org/deeplinks/2017/05/intels-management-engine-security-hazard-and-users-need-way-disable-it Accessed 22 January 2022.

Rijmenants, n.d..
Dirk Rijmenants, *One-time Pad* (n.d.). https://www.ciphermachinesandcryptology.com/en/onetimepad.htm Accessed 26th February 2022.

Roberts, 2013.
Dan Roberts and Spencer Ackerman, "Anger swells after NSA phone records court order revelations," *The Guardian* (June 2013). Accessed online on 17th February 2022.

Savage, 2013.
Charlie Savage, Edward Wyatt, and Peter Baker, "U.S. Confirms That It Gathers Online Data Overseas," *The New York Times* (June 2013). Accessed online on 17th February 2022.

Shah, 2022.
Agam Shah, "US House passes bill to boost chip manufacturing and

R&D," *The Register* (Feb 2022). Accessed online on 6th February 2022.

Signal, 2021.
Signal, *Grand jury subpoena for Signal user data, Central District of California (again!)* (October 2021). https://signal.org/bigbrother/cd-california-grand-jury/ Accessed 26 March 2022.

Talbot, 2009.
David Talbot, "China Cracks Down on Tor Anonymity Network," *MIT Technology Review* (Oct 2009).

The Federal Archives, n.d..
The Federal Archives, *About the Stasi Records Archive* (n.d.). https://www.stasi-unterlagen-archiv.de/en/archives/about-the-archives/ Accessed 2 April 2022.

Wallen, 2016.
Jack Wallen, "Is the Intel Management Engine a backdoor?" *TechRepublic* (July 2016). https://www.techrepublic.com/article/is-the-intel-management-engine-a-backdoor/ Accessed 25 March 2022.

Warren, 2021.
Tom Warren, "Why Windows 11 is forcing everyone to use TPM chips," *The Verge* (June 2021). https://www.theverge.com/2021/6/25/22550376/microsoft-windows-11-tpm-chips-requirement-security Accessed 25 March 2022.

Winter, 2012.
Philipp Winter and Stefan Lindskog, "How China Is Blocking Tor," *Karlstad University* (Apr 2012).

Wong, n.d..
Wing H. Wong, *Timing Attacks on RSA: Revealing Your Secrets through the Fourth Dimension* (n.d.). https://www.cs.sjsu.edu/faculty/stamp/students/article.html Accessed 25 March 2022.

Yadron, 2016.
Danny Yadron, Spencer Ackerman, and Sam Thielman, "Inside the FBI's encryption battle with Apple," *The Guardian* (Feb 2016). Accessed online on 25 March 2022.

Zhong et al, 2020.
Han-Sen Zhong et al, *Quantum computational advantage using photons* (2020). DOI: 10.1126/science.abe8770.