EUROPEAN COUNCIL ON FOREIGN RELATIONS
ecfr.eu

POLICY BRIEF

NO MIDDLE GROUND: MOVING ON FROM THE CRYPTO WARS

Stefan Soesanto

July 2018

SUMMARY

- Accepting a middle ground or finding a balanced solution on the issue of encryption is neither feasible nor, in fact, desirable.
- Privacy advocates and security researchers are destined to win the fight on stronger encryption and against key escrow, but they will lose the war on security – and most likely fragment along those fault lines in the not-so-distant future.
- In Europe, no single vision on how to tackle the challenges created by the rise of encryption currently exists on the political level.
- Law enforcement agencies in Europe view encryption as one among many other inter-related issues that are undermining their future role.
- From a European intelligence agency perspective, accepting the degradation and denial of intelligence collection efforts is an unacceptable solution to the encryption problem.
- A targeted approach, through the build-up arsenals of exploits, is the only alternative to backdoors, key escrow, and obliging companies to weaken encryption.

Introduction

Since the advent of the personal computer, the issue of government access to encrypted data has driven a wedge between law enforcement and the intelligence community on one side and privacy advocates and security researchers on the other.

In the so-called first crypto war, during the 1990s, privacy advocates and security researchers fought against comprehensive US export controls on cryptography and against deliberately weakening encryption. The war's outcome is largely responsible for the increased use and availability of encryption tools and for enabling the rise of e-commerce globally. Steven Levy, former chief technology correspondent at Newsweek, who literally wrote the book on the first crypto war in 2001, summarised the result in five words: "public crypto was our friend", meaning the US government's position shifted towards endorsing cryptography as beneficial to the wider public rather than solely viewing it as a threat to national security.

But 18 years after Jim Bidzos, founder of IT security conference RSA, declared that "the fight is over and our guys won", the world is embroiled in a second crypto war, which began with the Snowden leaks of 2013 and continues to the present day. The point of contention now is about allowing government agencies exceptional access to communications data and unlocking personal electronic devices.

To a degree, the same ethical questions as those in the 1990s are being discussed all over again. Should government agencies have access to encrypted data? How can they achieve this, technically, legally, and ethically? Should there be limits on how strong an encryption cipher can be? What security risks are governments willing to expose the general public to? And does the general public really need access to strong encryption in the first place? All these questions were answered 30 years ago. But, with technology continuously advancing and the threat landscape dynamically evolving, it is hardly a surprise that they have arisen again.

This paper aims first and foremost to avoid the mistakes of many other publications

that have tackled the issue of encryption. For example, the 2018 National Academy of Sciences' report, 'Decrypting the Encryption Debate: A Framework for Decision Makers', overwhelmingly focuses on how governments can achieve exceptional access, while the EastWest Institute's 2018 paper, 'Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions', sought to create common ground based on the status quo. In contrast, this paper will argue that accepting a middle ground or finding a balanced solution on the issue of encryption is neither feasible nor, in fact, desirable.

While privacy advocates and security researchers might rejoice reading those lines, this paper does not share their enthusiasm. In fact, it will show that, while privacy advocates and security researchers are destined to win the fight on stronger encryption and against key escrow, they will lose the war on security – and most likely fragment along those fault lines in the not-so-distant future.

To advance this argument and make it accessible to a wide audience, this paper adopts the following structure. First, it discusses the basics of the encryption problem, including a brief explainer about the difference between end-to-end and full-disk encryption, the "going dark/going spotty" debate, and the notions of "access versus risk" in the context of backdoors and key escrow. Second, alongside an overview of the state of the debate in the United States, the paper examines three areas that are central to understanding the dynamics around the encryption debate in Europe: European politics, European law enforcement, and the European intelligence community. And, finally, this paper will sketch out the course the issue is likely to follow going forward and conclude by articulating four policy recommendations for lawmakers to pursue.

Overall, this paper's main purpose is to dislodge the encryption debate from its current endless loop on strong encryption versus backdoors and key escrow, and lead to a rethink on the cost-benefit calculation that underpins the choices of today and the repercussions they might create ten years down the line.

What is encryption?

The basic features of cryptography – designing ciphers – have remained largely constant throughout history. Modern cryptography may appear to be a very different animal from the Spartan scytale (an early cryptographic device) or even the Enigma machines used by Germany during the second world war. Nonetheless, the goal remains the same: ensuring secrecy and security in communication.[1] The essential principles remain similar too: to encrypt a message, the plaintext (P) is encrypted with a secret key (K) to create the ciphertext (C). Decryption follows the reverse procedure: the ciphertext (C) is decrypted with the secret key (K) to produce the plaintext (P). A cipher, or algorithm, is therefore composed of two functions: encryption and decryption.

Over time, cryptographers have sought to develop more complex ciphers in order to better encrypt plaintexts, and cryptanalysts have in response searched for more intricate weaknesses in those ciphers. For example, in the ninth century Arab scholar Al-Kindi discovered the foundations of frequency analysis, based on his observation that certain letters and combinations of letters occur with varying frequencies in a written language.[2] A refined approach to frequency analysis eventually enabled English polymath Charles Babbage to break the Vigenère Cipher in 1854, 300 years after it was developed and gained notoriety as 'le chiffre indéchiffrable'.[3]By modern standards, classical ciphers such as the Vigenère Cipher are woefully insecure, because "they are limited to operations you can do in your head or on a piece of paper."[4]

One of the most important rules guiding modern cryptography is Kerckhoffs's principle, named after nineteenth century Dutch cryptographer Auguste Kerckhoffs. This states that "the security of the encryption scheme must depend only on the secrecy of the key (K), and not on the secrecy of the encryption algorithm."[5] In other words, even if the attacker knows exactly how the encryption algorithm works, they must be unable to discover the key to decipher the ciphertext.

For the cryptographic community this has translated into the best practice of openly publishing new encryption algorithms to allow for maximum scrutiny and to fix potential vulnerabilities – in line with the mantra 'make the cipher transparent, keep the key secure'. In the case of the Advanced Encryption Standard (AES), the US government followed this best practice rule. Rather than designing and commissioning its own standard cipher, the US National Institute for Standards and Technology opened up a public competition in 1997, asking for cipher proposals from the cryptographic community. Fifteen proposals were submitted, five finalists designated, and in 2001 the Rijndael cipher was selected to become the AES. Today, AES in its various key sizes (128, 192, and 256 bits) is used in most encryption products, including popular password managers, messenger applications, and hard-disk encryption software. Trying all possible combinations to find the key in a modern cipher such as AES-128, would take a trillion machines, each testing a billion keys per second, more than two billion years.[6]

However, none of this means that any implementation of AES is secure; far from it. In fact, there are numerous forms of attack that can and will be leveraged over time to exploit any weaknesses in the implementation of any cipher, including: side-channel attacks (such as changes in power consumption, changes in computational timing, or changes in sound); attacks against key generation systems; extracting keys from memory; "collision attacks"; targeting the end-points (such as mobile phones and computers); and exploiting sloppy password-creation habits.[7] A healthy dose of 'professional paranoia' is therefore essential when it comes to guarding against the countless attacks that have, will, and could be leveraged against a cryptographic

system now and in the future. As prominent cryptographers Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno pointedly put it: “If your cryptographic system can survive the paranoia model, it has at least a fighting chance of survival in the real world.”[8]

The bottom line is this: cryptography is hard – very hard. And there is currently no known way of testing whether a cipher is absolutely secure and will remain secure against all future attacks. The best-known solution to tackling this problem is to get as many researchers as possible to poke holes into a cipher and try to break its implementation. However, the same cryptographers also explain, “even with many seasoned eyes looking at the system, security deficiencies may not be uncovered for years.”[9] Therefore, the continuous development of ever stronger encryption ciphers is not a choice, it is a security need.

What are end-to-end encryption and full-disk encryption?

Kerckhoffs’s principle also states that key management is essential. This brings us to the difference between end-to-end encryption and full-disk encryption: full-disk encryption secures data-at-rest from unauthorised access, while end-to-end encryption secures data-in-transit from interception.

Key management is one of the factors that differentiates them. Full-disk encryption utilises symmetric encryption, in which the same key is used for both encryption and decryption. Matthew Green of Johns Hopkins University, explains this by noting that, “at boot time you enter a password. This is fed through a key derivation function to derive the cryptographic keys. If a hardware co-processor is available … your key is further strengthened by “tangling” it with some secrets stored in the hardware. This helps to lock encryption to a particular device.” In the case of BitLocker, a popular piece of encryption software, all keys are stored locally, with the exception of the USB key which can be used in lieu of the PIN.

End-to-end encryption is an asymmetric encryption scheme that creates two different keys: a public key for encryption and a private key for decryption.

Messenger applications, such as WhatsApp, Signal, and Telegram, use asymmetric encryption to "allow only the unique recipients of a message to decrypt it, and not anyone in between", – not even the service provider. *Wired*'s Andy Greenberg describes it thus: "Think of the system like a lockbox on your doorstep for the UPS delivery man: anyone with your public key can put something in the box and lock it, but only you have the private key to unlock it."

That said, symmetric and asymmetric encryption schemes are usually combined in order to build a secure communication system.[10] This means that, on its own, end-to-end encryption does nothing to secure the data on a device against unauthorised access, such as someone who knows its passcode, and full-disk encryption will not protect your data from interception if you send it from one device to another. Together, however, they can form a very secure communication system, which is of concern to law enforcement and intelligence agencies around the world.

Going dark and going spotty

Public discourse around encryption often portrays the matter as a zero-sum game: either one favours stronger encryption to better keep everyone secure, or one allows encryption to be weakened, which will make everyone less safe.

While it is correct that encryption nowadays protects everything from financial transactions and critical infrastructure to personal communications and health data, it is also true that, from a practical point of view, the average user has no idea how to encrypt an email or a hard drive, and is unaware of the security differences between "http" and "https" for securely processing credit card payments online. In part, this legacy failure stems from the success of the first crypto war. While companies confidently strode into the era of e-commerce, the average user was left largely alone to secure themselves.

The rise of mobile platforms, particularly the smartphone, offered a practical path to mitigate this legacy failure by allowing for an easier and more holistic implementation of encryption than on a personal computer. Apple's iOS 8, for instance, introduced full-disk encryption

in 2014. Windows 10 Home users, meanwhile, still have to download third party software to encrypt their hard drives (or upgrade to Windows Professional/Enterprise to enable the Bitlocker feature). Similarly, Facebook's move to enable end-to-end encryption by default for its 1.7 billion WhatsApp and Messenger users helped to better secure mobile phones, because of user preferences for communicating by mobile phone via instant messenger services rather than by email.

While almost all tech giants are continuously working towards stronger and more widespread use of encryption, BlackBerry outed itself in 2017 as one of the very few companies that might go as far as breaking its own encryption scheme if law enforcement agencies demand it do so. Despite this, most other technology companies have not followed BlackBerry, and so the widespread proliferation of easy-to-use encryption in the public domain has increasingly turned into a headache for policymakers, law enforcement agencies, and the intelligence community.

At the centre of the encryption debate is the issue of "going dark" or "going spotty." According to former FBI director James Comey, "going dark" refers to the phenomenon in which law enforcement personnel have the "legal authority to intercept and access communications and information pursuant to court order" but "lack the technical ability to do so." In contrast, "'going spotty'" describes the view that law enforcement and intelligence agencies have a wide spectrum of tools at their disposal to identify, surveil, and investigate a target or crime, but the increasing adoption of end-to-end and other forms of encryption is leading to a growth in intelligence blind spots.

The difference between both interpretations of reality is crucial to understanding the current encryption debate. Proponents stressing that law enforcement is going dark are viewing encryption as a threat to public order and national security. In contrast, the going spotty narrative focuses on the contribution public cryptography makes to the security of the general public – reminiscent of the outcomes of the first crypto war. As far as this paper is concerned, both views are correct and valid. The

fundamental problem is that both interpretations cannot be balanced or reconciled with each other to create common ground. The stakes are simply too high. If the director of the FBI is right, doing nothing to confront the encryption threat will increasingly endanger national security and undermine law and order. While, if the going spotty narrative is right, then doing nothing is the way to go.

Access versus risk

To partially solve the problem of going dark and going spotty, two potential solutions have taken centre stage over the past years: backdoors and key escrow.

Backdoors

Backdoors are deliberately built-in methods – or design oversights – that bypass the security of a cryptographic system and thereby allow a party to access encrypted information without authorisation. Backdoors can be either explicit or implicit. An explicit backdoor is anything from a hardcoded username/password combination, a code snippet that enables privileged rights, or the outright weakening of cryptographic standards by design requirements. Implicit backdoors, in contrast, exist theoretically, but lack a practical proof. Prominent examples include: Crypto AG, a Swiss company which has been accused of cooperating with Western intelligence agencies to supply foreign governments with cryptographic machines containing backdoors; and Dual EC DRBG, a pseudorandom number generator that was adopted as a standard by the US National Institute for Standards and Technology, despite the fact that it likely promulgating a backdoor for the National Security Agency.

Key escrow

Key escrow is a cryptographic key exchange process in which a copy of the private key is retained by a third party. The reasons for using such a system can range from wanting to easily recover lost keys and decrypting encrypted material in case a key is compromised to enabling third party access due to legal obligations.

The most notorious key escrow scheme is probably the Escrowed Encryption

Standard (EES) – better known by its Clipper chip – which was announced for implementation by the US government in 1993 but whose serious technical vulnerabilities soon became apparent. In 1996, the government ceased using EES; its encryption algorithm "Skipjack" was declassified and published by the NSA in 1998.

Even after the failure of EES, the idea of a scalable and secure key escrow scheme never really died. In its most recent rebirth, former chief technical officer at Microsoft, Ray Ozzie, put together his idea of a key escrow scheme named "Clear". However, this key escrow idea also soon collapsed under expert scrutiny and public pushback. Criticism centred on the inability of "manufacturers to secure massive amounts of extremely valuable key material against the strongest and most resourceful attackers on the planet." Numerous cryptographic experts pointed out other failures, such as: the lack of an absolutely secure processor that can handle an unbreakable police-only recovery mode. As one commentator put it: "if your proposal fundamentally relies on a secure lock that nobody can ever break, then it's on you to show me how to build that lock"; the possibility of an attacker "trick[ing] law enforcement into obtaining an unlocking key that purports to be for a criminal's phone but is actually for the phone belonging to someone else—say, Lockheed Martin's CEO—and this key would be relayed to the attacker"; and, the international problem of global operating companies storing private keys in foreign jurisdictions – such as a phone bought in China (that has keys stored in China) but used in the US – and how companies ought to handle access requests if the situation is reversed.

But assume for the moment that it is possible to build Ozzie's Clear key escrow scheme, solve all the technical problems, and nullify the risks of a security vulnerability ever occurring. Would this also solve the morally complex question of granting and trusting the government with the golden keys to access private communications? The answer is no – because a mere technical solution cannot solve a problem that is inherently political. Governments, law enforcement, and intelligence agencies may seek technical solutions to the issue of going dark/going spotty, but they still need also to solve the questions around trust.

The state of the debate in the US

In the US the encryption debate has largely been treading water since early 2016, when Comey went head to head with Apple's CEO Tim Cook over breaking into the iPhone 5C of one of the San Bernardino attackers. In a six-week-long legal battle, Apple's refusal to write alternative firmware to unlock the phone eventually led the government to pay $900,000 to Israeli mobile forensics firm Cellebrite, which successfully bypassed the iPhone 5C's security features.

Comey's successor, Christopher Wray, has replicated the agency's rhetorical push for access to encrypted data. In January 2018 he stressed that law enforcement's inability to crack encryption on mobile phones and other devices is "an urgent public safety issue." In high-profile remarks, Wray also noted that the FBI had been unable to access data from 7,775 encrypted devices over the preceding year, despite possessing legal permission to obtain the information. The consequences of going dark on these devices has, according to Wray, resulted in major setbacks in a number of cases related to counter-terrorism, human trafficking, and organised crime.

Following Wray's speech, the 7,775 figure has come under heavy scrutiny. It turned out that the FBI's calculation had combined three different databases, resulting in some devices being counted multiple times. According to the *Washington Post*, the number stands at between 1,000 and 2,000 devices. The blunder triggered a letter by Senator Ron Wyden (D-OR) asking the FBI to provide more information about the inflated numbers, while also stating that "when the FBI reportedly misstates the number of devices rendered inaccessible by encryption, it is either too sloppy in its work or pushing a legislative agenda." In January 2018 Wyden grilled Wray by asking outright for a list of cryptographers the FBI had consulted on what he dubbed "this ill-informed policy proposal." To date the FBI remains silent on this question. The senator did, however, receive a letter signed by four prominent cryptography experts who stressed that: "instead of vague proposals that sound reasonable yet lack details, the FBI needs to present the cryptographic research community with a detailed description of the technology that it would like implemented."

Wray's misstep has not been the only one to tarnish the encryption debate. In similar vein, speaking before the US Naval Academy in October 2017, deputy attorney general Rod Rosenstein argued: "if companies are permitted to create law-free zones for their customers, citizens should understand the consequences. When police cannot access evidence, crime cannot be solved. Criminals cannot be stopped and punished." In the same remarks, Rosenstein introduced the term "responsible encryption", which quickly became notorious among those closely involved in the encryption debate. The term ostensibly refers to a backdoor or a key escrow which law enforcement could leverage to decrypt data in conjunction with a warrant or court order.

Privacy advocates have been highly critical of the Rosenstein proposal. They believe that responsible encryption is merely a rebranded argument for law enforcement to gain exceptional access to communications data by significantly weakening encryption.

Cryptographers, cyber security experts, and the information security community at large subsequently picked apart Rosenstein's argument by noting that it offered very

few technical details on how responsible encryption would actually work in practice, and that Rosenstein had failed to address the fundamental security issues relating to backdoors and key escrow. Since then, little has changed in the US encryption debate or in US legislation.

The politics in Europe

In Europe, the string of terrorist attacks in Nice, Brussels, Paris, Berlin, Barcelona, Stockholm, and London prompted numerous European governments to raise the topic of backdoors, circumventing end-to-end encryption (law enforcement hacking), and weakening encryption standards upfront.

United Kingdom

After it emerged that the perpetrator of the March 2017 Westminster attack, Khalid Masood, had been using WhatsApp just minutes before he killed five people and injured 50, the then UK home secretary Amber Rudd argued that, "we need to make sure that organisations like WhatsApp, and there are plenty of others like that, do not provide a secret place for terrorists to communicate with each other." The same argument was echoed by prime minister Theresa May in early June the same year after the London Bridge attacks, which killed eight people and injured 48, when she called for the creation of international agreements that would "regulate cyberspace" and "deprive extremists of their safe spaces online." The online community mocked both sets of comments for their perceived ignorance of how end-to-end encryption and the internet work. The *Guardian*, for instance, ran with: "Backdoor access to WhatsApp? Rudd's call suggests a hazy grasp of encryption." Wired said: "Blaming the internet for terrorism misses the point."

A few months after the June attack, Rudd elaborated on the government's vision of encryption in an op-ed published by the *Daily Telegraph* in which she stated that "the government supports strong encryption and has no intention of banning end-to-end encryption," and is not asking companies to "break encryption or create so called back doors." Instead, Rudd essentially advocated for companies to make their

products less user-friendly by rhetorically asking "who uses WhatsApp because it is end-to-end encrypted, rather than because it is an incredibly user-friendly and cheap way of staying in touch with friends and family?"

In October, speaking at a meeting at the Conservative Party conference, the home secretary expressed frustration at the overwhelming criticism of the government's stance, and emphasised that she "doesn't need to understand how encryption works" to know that it is "helping criminals." But while it is true that no one ought to expect senior politicians like Rudd to understand all technicalities surrounding encryption, it is reasonable to at least expect her to listen to expert advice and develop her views based on evidence. In many ways, the home secretary was faced with the same conundrum as FBI director Wray. Rudd's successor, Sajid Javid, has so far remained silent on the specific issue of encryption, but has accused messenger app Telegram of being a "mouthpiece" for terror.

Germany

In Germany the encryption debate has been much more constrained publicly. The federal government's overarching position rests on an economic and a security pillar.

The "Digital Agenda 2014-2017" sets out an economic foundation for the future, by emphasising the need to "support the use of more and better encryption and aim [for Germany] to be the world's leading country in this area." To realise this, in November 2015 the encryption focus group overseen by the federal interior ministry developed a non-binding charter which outlines seven basic principles, including: raising awareness of end-to-end encryption; ensuring user-friendliness; developing trust certificates; and providing continuous innovation. At the time of writing, the charter has a mere 21 signatories – 11 more than two and a half years ago.

Germany's crypto policy, which dates back to 1999, stipulates its security goal by stating that while "there will be no ban or limitation on crypto products, [...] law enforcement and security agencies shall not be weakened by the widespread use of encryption." To maintain this goal in the age of end-to-end encryption, in mid-June

2017 federal and state interior ministers reached unanimous agreement to monitor messenger services, such as WhatsApp, for the purpose of fighting terrorism – "monitor" in this case means reading the plaintext, rather than merely looking at data traffic. Then federal interior minister Thomas de Maizière explained the decision by arguing that "it cannot be that there are law-free areas when it comes to the prosecution of crimes." In late June the German parliament passed a new law to make criminal procedures more effective by specifically allowing German law enforcement agencies to deploy spyware (the so called Remote Communication Interception Software or Staatstrojaner) to circumvent end-to-end encryption on mobile devices in both terrorism and criminal investigations. To fulfil this mandate on the technical end, in September 2017 the interior ministry launched the Central Office for Information Technology in the Security Sector (ZITiS), whose mission is to "advance the development of technical tools used by all security authorities in the fight against crime at [sic] one place," and to "identify new trends and developments, and prepare for the future by developing counter-measures."

Privacy advocates and security researchers view these developments with extreme concern, as they see them as a build-up phase for creating an arsenal of trojans that will be leveraged for state hacking purposes. Frank Garbsch, spokesperson for the Chaos Computer Club, for example, noted that: "to sell state hacking as just another surveillance measure like any other is … a brazen distortion of the truth." Garbsch is right. Developing malware that can compromise a specific device and thereby intercept messages before they are encrypted, or after they have been read, is a security threat for every user owning the same device model and software configuration. However, the German government's approach is a working solution to circumvent encryption without weakening or breaking it. And it will also not violate privacy if it is targeted and lawfully implemented.

France

In August 2016, Germany's interior minister promoted elements of Berlin's approach to encryption when he met with then French interior minister Bernard Cazeneuve in

Paris. The meeting essentially kickstarted a coordinated Franco-German effort aimed at pushing the European Commission to draft a new regulation that would oblige mobile messaging service operators to cooperate with law enforcement in terrorism-related investigations. While singling out Telegram, Cazeneuve stressed that: "if such legislation was adopted, this would allow us to impose obligations at the European level on non-cooperative operators." Cazeneuve and de Maizière certainly had a valid point, given that Telegram has consistently refused to block the Islamic State group and other jihadist organisations from using its platform. Other messenger service operators, particularly those located outside the European Union, have also been extremely slow to comply and to share metadata and other valuable intelligence with law enforcement agencies. The problem with this approach is that both Russia and Iran have unsuccessfully tried to make Telegram comply with access and censorship demands, before banning the app in April 2018. In Russia's case, local internet service providers inevitably blocked 15.8 million IPs on Amazon's and Google's cloud platforms, which Telegram used to domain-front its traffic to Russia, causing collateral damage in the process and disconnecting Russia from part of the internet infrastructure. As Telegram founder Pavel Durov put it at the time: "threats to block Telegram unless it gives up private data of its users won't bear fruit. Telegram will stand for freedom and privacy." The clash is a vivid reminder that messenger services run on third-party infrastructure and that they will attempt to find ways to redirect traffic through alternatives routes. Blocking them is simply not a feasible way to ensure compliance.

In France, the debate on encryption has slowly begun to resemble that in the UK. In April 2017, then presidential candidate Emmanuel Macron expressed his determination to crack down on terrorism by energetically proclaiming that "until now, big internet companies have refused to give their encryption keys or access to this content, saying that they have told their clients that their communications are encrypted. This situation is no longer acceptable." After being elected president, Macron highlighted the issue again when he met with May in mid-June, stating that "we want to improve access to encrypted content under conditions which preserve

the confidentiality of the correspondence so that these message applications cannot be used as tools for terrorists or criminals." How exactly the French government intends to do this remains woefully unclear. In many ways this echoes the "responsible encryption" fiasco Rosenstein tried to push in the US.

Macron's rhetoric also prompted the National Digital Council (CNNum) to send a letter to interior minister Gérard Collomb, stressing that "encryption is a vital tool for online security" and that CNNum is "particularly concerned about the government's security trajectory" on digital issues. But the French government knows exactly how important encryption is. During the presidential campaign, Macron and his inner circle grew very fond of Telegram because they wanted "to use an encrypted messaging service that even his rivals in the last government could not crack." And, according to Reuters, "since then, most of his lawmakers have joined the app and the president himself can often be seen online on Telegram, sometimes in the early hours of the morning."

It is important to note in this context that the French government's move against mobile messaging service operators, and specifically Telegram, relates to its own geopolitical and economic interest. French security services were rightly worried that the Russian government might one day compel Telegram to hand over its encryption keys. The French government has also long advocated for data sovereignty laws, which would require tech companies to store data from French citizens inside France. So it should not come as a surprise that the move against Telegram coincided with the French government developing an as-yet-unnamed French-made end-to-end encrypted messenger app that will be "internal to the state and intended to replace" non-state services used by parliamentarians and ministers. Whether this app will ever be made available to all French citizens is still unclear.

European Union

In early 2017, Cazeneuve and de Maizière sent a letter to the European Commission calling for new legislation to allow greater sharing of personal information between police forces and demanding that technology companies devise encryption systems

that are both secure and accessible to law enforcement. Numerous media outlets, privacy advocates, and even security vendors interpreted this as a step in the wrong direction. Some even saw in it an attempt to ban, limit, or weaken encryption in messenger apps altogether. The European Digital Right association (EDRi), for instance, noted that Berlin and Paris were "fighting terrorism by weakening encryption." Voice of America said that both countries are "push[ing] for EU encryption limits", and Kaspersky's ThreatPost even proclaimed that France and Germany called for a "European decryption law."

Following media reports suggesting that the European Commission is also working on a proposal to tackle encryption, a spokesperson had to explain that "on encryption the discussions are still ongoing. And for now there is no legislative plan." In the meantime, de Maizière's call for "very limited possibilities for decrypting encrypted communication" largely fell on deaf ears. The irony of the entire episode was that to a large extent both ministers were echoing the recommendations made by Europol and the European Network Information Security Agency (ENISA) only three months prior, which emphasised the need to "intensify the exchange of best practices and innovative ideas on the management of encrypted communication [to] minimize the obstacles facing national defence authorities in the fight against terrorism," and called for "the fostering of close cooperation with industry partners, as well as the research community with expertise in crypto-analyses for the breaking of encryption where lawfully indicated." The major difference from the French-German letter was that Europol and ENISA provided additional context (by highlighting the benefits of strong encryption), came out against backdoors and key escrow, and advocated for a "solution that strikes a sensible and workable balance between individual rights and protection of EU citizen's security interests." If de Maizière and Cazeneuve had only framed their proposal more adequately, it most likely would not have been perceived as a ban, limit, or attempt to weaken encryption.

After the persistent Franco-German demands for new legislation, in October 2017 Julian King, commissioner for the security union, announced a number of initiatives to fund more police training to crack encryption technology. "Some member states

are more equipped technically to do that than others. We want to make sure no member state is at a disadvantage," said King. To fill this gap, the European Commission wants Europol to coordinate a new network of national law enforcement experts on encryption, and has promised an extra €500,000 for police training in 2018.To encourage member states to share decryption expertise across regions and borders, the European Commission also envisions the development of a common toolbox for alternative techniques that law enforcement agencies can use to obtain information without weakening encryption at a more general level.

Despite the disavowal of backdoors, some observers were again quick to express criticism of the European Commission's approach. Dutch Liberal MEP Marietje Schaake commented that the "Commission wants to have its cake & eat it too: toolbox to break encryption… Without weakening encryption." Others noted that, from a practical point of view, it is highly unlikely that law enforcement agencies will be able to crack strong encryption schemes present on devices and in messenger services. And it even seems less likely that law enforcement agencies in one country would be willing to share their encryption-cracking tools and expertise with others.

Meanwhile, in June 2017 the European Parliament's committee on civil liberties, justice, and home affairs, (LIBE) circulated a draft report, which proposed banning backdoors and making encrypted data untouchable, arguing that "when encryption of electronic communications data is used, decryption, reverse engineering or monitoring of such communications shall be prohibited." The draft report even went so far as to stipulate that "Member States shall not impose any obligations on electronic communications service providers that would result in the weakening of the security and encryption of their networks and services." In the final report, the former statement was amended to "when encryption of electronic communications data is used, decryption by anybody else than the user shall be prohibited," which is a more careful phrasing as it will allow law enforcement agencies to reverse-engineer and monitor encrypted traffic. The latter, however, still stands in its original form and was entered into inter-institutional negotiations in late 2017. Depending on the outcome of the negotiation, the LIBE committee's report could end up pressuring EU

governments to abolish any ideas on backdoors and key escrow – which privacy advocates and security researcher will welcome – while at the same time substantially narrowing public-private cooperation – which law enforcement will stringently oppose.

The Netherlands

The approach taken by the Dutch government comes closest to what the draft LIBE report was initially trying to advocate. In January 2016, the Dutch adopted a whole-of-government approach, which embraces strong encryption and denounces any kind of backdoor. In a letter to the Dutch parliament, security minister Ard van der Steur explained that "the cabinet endorses the importance of strong encryption for internet security" and that "at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands."

However, this does not mean that Dutch law enforcement is unable to obtain encrypted data or break into hardware and software products. Quite the contrary: in the same month that the Dutch government adopted its whole-of-government approach, the Netherlands Forensic Institute (NFI), a body that assists law enforcement in forensic evidence retrieval, confirmed to Motherboard that they "are capable of obtaining encrypted data from BlackBerry PGP devices." According to the initial report by Crimesite.nl, the NFI was able to siphon 85 percent of data from two BlackBerry PGP phones confiscated in a criminal case. Similarly, in November 2016 the Dutch government approved a bill that allows its police and intelligence agencies to exploit both known and unknown hardware and software vulnerabilities to "guarantee national security and to detect criminal offenses." Because of the contentious nature of the bill, the ruling government coalition was forced to attach an amendment which requires law enforcement agencies to either report the vulnerability to the affected vendor after it has been used, or, if they want to retain the vulnerability for other operations, to seek approval through an independent court review.

Privacy and security researchers have condemned the Dutch government's stance. The European Digital Rights association (EDRi) even went so far as to argue that "any vulnerability should be patched immediately," and that the government "ignores the fact that those vulnerabilities may be acquired on the black market, or that they may be shared amongst intelligence services." To a certain degree the EDRi is correct, particularly if one defines an unknown vulnerability as an implicit backdoor. Yet Dutch government agencies are not the creators of said vulnerabilities or backdoors – vendors are – and their exploitation may not always work – as the BlackBerry PGP example showed.

Given the political discrepancies on encryption across the EU – ranging from advocating for backdoors/key escrow, circumventing encryption, and weakening encryption standards – it is important to recall that the discussion in the US is neither more advanced nor any more coherent. In fact, speaking at the 2017 Aspen Security Forum, Dana Boente, then acting assistant US attorney general for national security, even went so far as to argue that "the terrorism challenges in Europe are really kind of tough, and [the Europeans] may lead the way and carry some of our water on this."

Law enforcement in Europe

Whether EU member states can actually carry some water will depend to a large extent on the ability of European law enforcement agencies and relevant ministries to articulate a coherent vision of the encryption challenge. But, as outlined above, no single vision currently exists in the political realm.

To date, the most comprehensive open source data available on the nature of the encryption problem as it relates to law enforcement is a questionnaire sent by the Council of the European Union to the justice ministers of 25 EU member states in September 2016. The Council designed the questionnaire in order to "map the situation and identify the obstacles faced by law enforcement authorities when gathering or securing encrypted e-evidence for the purposes of criminal proceedings." Thanks to a freedom of information act request by the Dutch NGO Bits

of Freedom, full public access was granted to the questionnaire answers of 19 member states and partial access to the input of one member state. Five member states – Belgium, Bulgaria, France, Malta, and Portugal – refused access to their questionnaires, citing security reasons.

Overall the data reveals sharp national discrepancies across practical, financial, personnel, technical, and legal barriers. For instance, to the question "How often do you encounter encryption in your operational activities?" the UK, Latvia, and Lithuania answered "almost always", Hungary, Slovenia, and the Czech Republic replied "rarely", while Germany explained that it "does not compile statistics as to the occurrence of encryption." When it comes to "the main types of encryption mostly encountered during criminal investigations", the answers unsurprisingly included everything from encrypted emails (PGP/GPG), HTTPS, SFTP, P2P, Tor, SSH tunnelling, and full-disk encryption, to messenger apps, data stored in the cloud, and data on mobile devices. Yet national distinctions were clearly visible, with Polish law enforcement stating that it was primarily dealing with email encryption and messenger services, while in Sweden SSH tunnelling and Tor topped the list.

National laws are equally fragmented across the EU, particularly as concerns the obligation of service providers to provide law enforcement agencies with encryption keys and passwords. In Germany, "providers of telecommunication services may be ordered to disclose passwords or access codes to the authorities as far as they have stored such passwords or access codes." In Latvia, cooperation occurs on a voluntary basis, while in Austria service providers are protected by the principle of confidentiality of communication and data protection rules. In Romania, in contrast, there is no specific legislation on encryption, meaning that "no person [or company] in possession of devices/e-data is legally obliged to make them available to law enforcement."

Faced with these divergences, it should come as no surprise that the main issues facing law enforcement agencies across Europe include: national legal limitations; non-cooperative service providers (particularly those located outside Europe); time

constraints on decrypting files due to data retention policies and unbreakable encryption schemes; the procurement of expensive tools and computing equipment; gaining access to third party resources or software; and hiring law enforcement personnel with practical decryption experience.

Despite their differences, the various agencies have put forward strikingly similar solutions. The Germans, for example, note that "with sufficient resources, many new and innovative approaches can be leveraged to mitigate the detrimental effect of encrypted data on criminal investigations." The Dutch echo this call but also warn that "other means to get access to devices is also getting harder and harder." Overall, most law enforcement agencies stress the need to modernise applicable laws and oblige companies to work with law enforcement in the country where they offer their services. Many also highlighted the need for more financial resources to up the ante on the technical and personnel side.

At the EU level, agencies specifically highlighted: the need to improve technical expertise (including how to handle e-evidence); the need for a platform to streamline the exchange of best practices; and the need for a clear legal framework concerning law enforcement hacking and interception of electronic evidence on devices before it is encrypted.

On the specific issue of backdoors and key escrow, for example, only Romania expressed a desire for "mandatory key encryption disclosure for service providers, including social service providers [such] as Skype, WhatsApp, etc." The UK's response, in contrast, largely rested on the Investigatory Powers Act (IPA), which includes a mechanism that would "require operators to remove encryption where it is reasonably practicable and technically feasible to do so." However, in April 2018, the UK High Court of Justice declared the IPA unlawful, because its data retention component was deemed incompatible with EU law. It therefore remains to be seen how the IPA, once it comes into force, will actually function in practice.

In contrast to the political discourse, law enforcement agencies in Europe view encryption as one among many other inter-related issues that are undermining the

future role of law enforcement in an increasingly interconnected, rapidly evolving digital world.

Intelligence agencies in Europe

The mission of every signals intelligence agency is to provide decision-makers with an information advantage, protecting the country and keeping the public secure. Defeating encryption is a vital part of this mission, whether it pertains to foreign intelligence collection, counter-intelligence efforts, or the fight against terrorism and organised crime. Indeed, every intelligence effort, including breaking the Enigma code during the second world war, or the NSA's signals intelligence operations exposed by Edward Snowden in 2013, are conducted in support of national security and defence efforts. As former NSA and CIA director General Michael Hayden tellingly put it, "the world is not getting any safer, and espionage remains our first line of defense."[11]

In Germany, the foreign intelligence service (BND) is extremely worried about the increasing adoption of end-to-end encryption in messenger services. According to classified documents obtained by Netzpolitik.org in November 2016, the agency is only able to monitor 10 out of 70 messenger services in use, which significantly hampers the BND's signal intelligence collection efforts. To overcome these blind spots, the BND requested an extra €73m in 2017, to set up project Panos, which would work to find weaknesses in messenger apps to circumvent end-to-end encryption. In addition, the leaked documents also reveal that the agency requested additional funding to buy expertise from external companies and service providers to help decrypt data and to break into devices.

Bernard Barbier, then technical director at France's intelligence agency DGSE, candidly explained in 2013 that its "main targets today are no longer government or military encryption, because 90% of our work focuses on anti-terrorism. … Today, our targets are the networks of the public at large, because they are used by terrorists."

Equally in the Netherlands, Rob Bertholee, head of the Dutch intelligence and security

service AIVD, expressed concerns about the Dutch government's stance on encryption, arguing that the Netherlands would be better off restricting encryption on chat services like WhatsApp and Telegram as much as possible rather than "accept[ing] that we are no longer able to read the communication of terrorists."

Meanwhile, former GCHQ director Robert Hannigan stressed in an interview with the BBC that "[we] cannot uninvent end-to-end encryption," and that "[we] cannot legislate it away." Even "trying to weaken the system or trying to build in backdoors won't work" either. Instead, Hannigan put his money on building stronger cooperation between service providers and government agencies, to circumvent encryption by "getting to the end point, whether it is the smartphone or the laptop, that somebody who is abusing encryption is using."

Ironically, Hannigan's position perfectly aligns with the views held by UK law enforcement but stands in remarkable contrast to GCHQ's own efforts to weaken and break encryption schemes. According to the 2015 UK Parliament Intelligence and Security Committee report on privacy and security, "terrorists, criminals and hostile states increasingly use encryption to protect their communications. The ability to decrypt these communications is core to GCHQ's work, and therefore they have designed a programme of work – [redacted] – to enable them to read encrypted communications." Indeed, the Snowden leaks confirmed the existence of a decryption program named Edgehill, which is aimed at "cracking encryption used by 15 major internet companies and 300 virtual private networks."

Privacy advocates in Europe and beyond have interpreted the recent efforts of the intelligence community as destabilising and counter-productive. In June 2017, for example, 65 privacy groups, ranging from Amnesty International and Human Rights Watch to the Electronic Frontier Foundation and the Tor Project, drafted a joint letter to "the Ministers responsible for the Five Eyes Security Community," stating that even engaging in discussions to "press technology firms to share encrypted data with security agencies in hopes to achieve a common position on the extent of … legally imposed obligations on … device-makers and social media companies to cooperate"

threatens the "integrity and security of general purpose communications tools and would be detrimental to international commerce, the free press, governments, human rights advocates, and individuals around the world."

While it is commendable that privacy advocates are speaking out on behalf of the rights and cybersecurity interests of all internet users, the fact remains that national intelligence agencies are not tasked with upholding global stability, nor is it their job to safeguard the rights and cybersecurity interests of foreign citizens living abroad. From an intelligence agency perspective, accepting the degradation and denial of intelligence collection efforts is an unacceptable solution to the encryption problem, as it would endanger national security and defence efforts.

The "gray market"

Complicating the current discourse on encryption is also the increasing propensity of government agencies to approach third party companies that sell technical solutions to circumvent encryption.

The most well-known example is Cellebrite. But there are many more companies that operate in this grey market, something which contributes to a more proactive solution to tackling the going dark/going spotty problem, but which also opens up a tinderbox on the security side.

Digital forensics firm Grayshift, for instance, is currently selling the Graykey – a 4x4 box with two lightning cables to plug-in iPhones. For a mere $15,000 the Graykey is able to leverage yet unknown security vulnerabilities in up-to-date iPhones, including the newest model, the iPhone X. According to Joseph Cox at Vice Motherboard, "the Maryland State Police and Indiana State Police have procured the technology; local police forces have indicated they may have purchased the tool; other forces have received quotes from Grayshift; the DEA is interested in sourcing GrayKey; the Secret Service plans to buy six of the boxes; and that the State Department has bought GrayKey." So far, it seems that Grayshift is only selling its products in the US.

Hacking Team, a company based in Italy is probably the most notorious player in the field. Founded in 2003, it created a program called Ettercap, which could monitor and remotely manipulate target computers. Milan's police department was one of their its government customers, not only buying Ettercap but also urging the company to write a Windows driver that would enable them to listen in to a target's Skype call. By 2015, Hacking Team employed 40 people and sold commercial hacking software to law enforcement agencies in "several dozen countries" on "six continents", and even provided them with custom features, regular updates, and tech support. The year 2015, however, also marked Hacking Team's temporary downfall, as it fell victim itself to hackers who posted 400GB of secret source code and internal data online. The leak revealed that Hacking Team was not only selling its products to law enforcement and intelligence agencies in NATO countries, but also to authoritarian governments across the globe, including those hostile to the US. Today, Hacking Team is still alive and kicking thanks to a wealthy investor from Saudi Arabia. According to its website, its "Remote Control System, is used by 50+ major governmental institutions for critical investigations, in more than 35 countries."

In contrast to the aforementioned examples, Zerodium, a US-based start-up, is relying on bug-bounty programs to source zero-day exploits from security researchers. In September 2015, Zerodium ran the largest bug bounty award competition ever, called 'The Million Dollar iOS 9 Bug Bounty,' which was paid out a few weeks later to an anonymous team of hackers. Zerodium's founder Chaouki Bekrar confirmed to *Wired* that the company "plans to reveal the technical details of the technique to its customers, whom the company has described as 'major corporations in defense, technology, and finance' seeking zero-day attack protection as well as 'government organizations in need of specific and tailored cybersecurity capabilities.'" According to Zerodium's latest figures, the company is willing to pay up to $1.5m for an iPhone remote jailbreak, up to $500,000 for a remote code execution in any of the popular messenger apps, and up to $300,000 for a remote code execution in Windows 10. Writing for the *Register* in April 2018, journalist Iain Thomson commented that: "barely a decade ago the mere idea of selling

vulnerabilities was highly controversial. Today the market is mature, but increasingly complicated - researchers can now choose between making lots of money, being moral and making less, or going fully black."

Future dynamics

First, the US and European governments will lose the encryption debate – because of the absence of a viable technical and feasible political solution – and will inevitably resort to treating tech companies as non-cooperative actors that undermine national security. Second, in the short term, government agencies will increasingly turn inward while purchasing exploit kits from third party companies to circumvent encryption. In the long term, government agencies will, on a technical level, cooperate more closely domestically (namely, through convergence between law enforcement and intelligence agencies) and across national borders (by partnering with government agencies abroad). Third, the vulnerability market will increasingly be distorted, with governments paying handsomely for vulnerabilities and exploit kits, pricing out traditional bug-bounty programmes, and changing the dynamics for responsible vulnerability disclosure. Fourth, the natural alliance between privacy advocates and security researchers will shatter: privacy advocates will endorse the government's targeted approach to circumventing encryption to combat crime, while security researchers will rail against government agencies exploiting and withholding knowledge of vulnerabilities in common software and hardware. And it remains unclear what might happen if government agencies lose their exploit kits to a hostile nation state or cyber criminal group. And, fifth, users will be the biggest losers. They will feel obliged to purchase ever more secure and expensive devices while government agencies devote more and more resources – taxpayer money – to breaking into them.

As outlined at the beginning of this paper, the encryption debate is, at its core, largely about either strengthening encryption or weakening encryption – and, so far, strengthening encryption has won every argument. However, if contrasted to the scenario outlined above, the cost-benefit analysis for continuously strengthening

encryption is no longer clear-cut. It might even have the opposite effect, by making the world much less secure than allowing encryption to weaken. In sum, the current public discourse has largely focused on the mostly positive outcomes of the first crypto war, but ignores the dangers and substantial costs if governments take an alternative approach to solve the going dark/going spotty problem.

Recommendations

To move the current encryption debate forward, stakeholders ought to recognise two core elements of the situation.

First, encryption – specifically, end-to-end encryption – is here to stay. It is not going to disappear and nor will any new solution emerge to allow law enforcement and intelligence agencies exceptional access to encrypted data.

Second, there is no middle ground. A targeted approach is the only alternative to backdoors, key escrow schemes, and obliging companies to weaken encryption. This means that law enforcement and intelligence agencies need to have the resources, tools, and legal framework needed to hack into computers and mobile devices, obtain private encryption keys and data before it is encrypted, and have the technical and legal means to break into an encrypted device if they have physical access to it. This strategy will naturally necessitate that the agencies be well funded, well staffed, and allowed to build up an arsenal of exploits to break into devices.

In relation to this, policymakers should consider the following recommendations:

- Ministries of the interior, justice, and defence need to create a transparent framework for broad hacking powers. These should: allow for targeted hacking strategies that can be approved at short notice; enable the retention and constant flow of exploits to penetrate a wide set of devices, products, and services; and ensure that toolkits can be legally purchased and shared. It will doubtless remain difficult to square the circle between law enforcement hacking domestically and the work of intelligence agencies breaking encryption schemes

to gain access to signals intelligence abroad. At its core, the prospective solution will inevitably have to incorporate a government agency that links law enforcement agencies and the intelligence community on a technical level. However, rather than having each EU member state set up its own agency and then network between them, it might be more prudent to centralise this technical cooperation within a new EU agency to ensure legal oversight.

- European policymakers should allow law enforcement and intelligence officials to take the lead in the public debate on encryption. Europe simply cannot afford a situation in which highly technical issues are discussed by political appointees who have little knowledge of the intricacies at work and are seeking to score political points by appearing strong on the rule of law. In particular, intelligence agencies across Europe need to overhaul their communication strategies. Currently, the intelligence community is losing both effectiveness and legitimacy through its inability and unwillingness to explain to the public its crucial role in addressing foreign and domestic threats. Equally, law enforcement agencies need to start to collect, disseminate, and share empirical evidence that will: guide the public debate on and need for law enforcement hacking; support the transparent adoption of, and discourse on, future policies; and, swiftly identify emerging challenges and adequate responses.
- The European Commission should speed up the collection of good practices to streamline law enforcement hacking. Harmonising legal frameworks should not necessarily be at the top of the agenda. Instead, the European Commission ought to engage with law enforcement agencies and national governments to implement solutions that tackle technical, financial, and capacity problems directly.
- The European Parliament should avoid creating privacy policies that box in the encryption debate. Language that hints at the outlawing of decryption techniques, such as breaking insecure hash functions and bruteforcing passphrases, is the last thing law enforcement agencies need in their fight against terrorism and cyber crime.

Acknowledgements

I would like to thank Teodora Delcheva for her amazing research support, proof-reading the draft paper, and being an integral member of the cybersecurity & defence team at ECFR. Special thanks also to Adam Harrison for his editing wizardry and pushing me over weeks, if not months, to make this paper better, richer in details, and accessible to a non-tech audience.

Thanks also to Susi Dennison and Jeremy Shapiro for their continuous support and offer to publish this policy brief at ECFR. And thanks to Maria Isidro for allowing me to present a draft of this paper at the Cloud Security Expo 2018. A big shout-out also to the team at Access Info Europe for their great work on asktheeu.org.

Biography

Stefan Soesanto is the former Cybersecurity & Defence Fellow at the European Council on Foreign Relations (ECFR) and a non-resident James A. Kelly Fellow at Pacific Forum.

At ECFR, he designed and held a cyber wargame exercise in cooperation with Microsoft and organised the Odense Cybersecurity & Defence Conference together with the Center for War Studies at the University of Southern Denmark and the Office of the Danish Tech Ambassador.

Prior to his role at ECFR, Soesanto served as a research assistant at RAND Europe's Brussels office, co-authoring reports for the Civil Liberties, Justice, and Home Affairs Committee in the European Parliament "Cybersecurity in the European Union and Beyond: Exploring Threats and Policy Responses", and a "Good Practice Guide on Vulnerability Disclosure" for the European Network Information Security Agency (ENISA). He also assisted in the project on "Investing in Cybersecurity" for the Dutch Ministry of Justice and Security.

Stefan holds an MA from Yonsei University (South Korea) with a focus on security

policies, and international law, and a BA from the Ruhr-University Bochum (Germany) in political science and Japanese.

FOOTNOTES

[1] Simon Singh. 1999. The Code Book – The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Fourth Estate, p. ix

[2] Simon Singh. 1999. The Code Book – The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Fourth Estate, p. 17-25

[3] Simon Singh. 1999. The Code Book – The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Fourth Estate, p. 45-78

[4] Jean-Philippe Aumasson. 2018. Serious Cryptography – A Practical Introduction to Modern Encryption. No Starch Press, p. 7

[5] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. 2010. Cryptography Engineering – Design Principles and Practical Applications. Wiley Publishing, p. 24

[6]For a flash animation on how AES works see: https://www.youtube.com/watch?v=mlzxpkdXP58.

[7] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. 2010. Cryptography Engineering – Design Principles and Practical Applications. Wiley Publishing, p. 33-35; 54-56.

[8] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. 2010. Cryptography Engineering – Design Principles and Practical Applications. Wiley Publishing, p. 8

[9] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. 2010. Cryptography Engineering – Design Principles and Practical Applications. Wiley Publishing, p. 13

[10] Jean-Philippe Aumasson. 2018. Serious Cryptography – A Practical Introduction to Modern Encryption. No Starch Press, p. 15.

[11] Michael V Hayden. 2016. “Playing to the Edge: American Intelligence in the Age of Terror,” p. xiv.

ABOUT ECFR

The European Council on Foreign Relations (ECFR) is the first pan-European think-tank. Launched in October 2007, its objective is to conduct research and promote informed debate across Europe on the development

of coherent, effective and values-based European foreign policy. ECFR has developed a strategy with three distinctive elements that define its activities:

- A pan-European Council. ECFR has brought together a distinguished Council of over two hundred Members – politicians, decision makers, thinkers and business people from the EU's member states and candidate countries – which meets once a year as a full body. Through geographical and thematic task forces, members provide ECFR staff with advice and feedback on policy ideas and help with ECFR's activities within their own countries. The Council is chaired by Carl Bildt, Emma Bonino and Mabel van Oranje.
- A physical presence in the main EU member states. ECFR, uniquely among European think-tanks, has offices in Berlin, London, Madrid, Paris, Rome, Sofia and Warsaw. Our offices are platforms for research, debate, advocacy and communications.
- Developing contagious ideas that get people talking. ECFR has brought together a team of distinguished researchers and practitioners from all over Europe to carry out innovative research and policy development projects with a pan-European focus. ECFR produces original research; publishes policy reports; hosts private meetings, public debates, and "friends of ECFR" gatherings in EU capitals; and reaches out to strategic media outlets.

ECFR is a registered charity funded by the Open Society Foundations and other generous foundations, individuals and corporate entities. These donors allow us to publish our ideas and advocate for a values-based EU foreign policy. ECFR works in partnership with other think tanks and organisations but does not make grants to individuals or institutions. www.ecfr.eu

 ISBN: 978-1-911544-63-0. Published by the European Council on Foreign Relations (ECFR), 4th Floor,

Tennyson House, 159-165 Great Portland Street, London London W1W 5PA,
United Kingdom