University of St Andrews | FOUNDED 1413

The Handa Centre for the Study of Terrorism and Political Violence

CSTPV Occasional Papers

End-to-End Encryption and Counterterrorism – Untying the Gordian Knot with State Hacking?

Lotta Rahlf

Abstract

While the increasing possibilities for end-to-end encrypted communication constitute a technical advance for general data protection, new challenges arise for law enforcement and intelligence agencies in monitoring terrorist communications. To work around the problem of terrorists 'going dark' and evading authorities' surveillance, German authorities have come to employ controversial methods of communications interception through equipment interference using state spyware. In this paper, I reflect on the proportionality of such measures in light of their implications for fundamental rights by discussing theoretical and practical problems. I thereby constructively explore a current Gordian knot in counterterrorism in the digital age.

1. Terrorism 'Going Dark'

Lawful interception refers to the selective monitoring and collecting of communications data by state authorities, such as law enforcement and intelligence agencies, under a designated legal framework. What is sometimes also referred to as governmental 'wiretapping' has a long and complex technological and political history (Fitsanakis 2020). Throughout, it has been particularly central to counterterrorism efforts, both in preventing acts of terror as well as in tracking down perpetrators and their networks (Denning and Baugh 1999, 252). However, the days when state authorities' counterterrorism needs and capabilities were confined to the interception of telephone conversations are long bygone, primarily due to ongoing technological developments: As interpersonal telecommunication increasingly shifts to social media forums or private chats, new opportunities for terrorist communication beyond traditional communication techniques arise. While this primarily necessitates law enforcement and intelligence agencies to expand their activities to the online environment, they must furthermore adjust to ongoing technical innovations in this virtual space. One particular challenge to the previous parameters of communications surveillance is the development and increased availability of end-to-end encrypted communication services.

Encryption is based on the idea of protecting an exchange of data or information through an encoding-decoding process that is only accessible to selected individuals. However, the distinctive feature of end-to-end encryption is that only the recipient has a private key to decrypt the message received, thus preventing third parties from accessing the data exchange (Graham 2016, 20). In principle, this is an innovation of benefit to all internet users, constituting an essential security feature for information infrastructure, including data, payment, and communications traffic (Denning and Baugh 1999, 251). At the same time, blocking third-party access to communications on social media has significant implications for their interception by law enforcement and intelligence agencies. If these state authorities were to monitor an end-to-end encrypted interpersonal communication using hitherto standard wiretapping practice, messages would only appear as 'scrambled information known as ciphertext' (B. Kerr and Schneier 2018, 990–91).

Consequently, while the technological innovation of end-to-end encryption has improved all internet users' information security and digital transactions, it equally serves as a strategic benefit to criminals, including terrorists. Although the possibility of encrypting terrorist communication with specific software had existed for some time, it required significant technical expertise and resources. Thus, the fact that various messaging platforms, such as Telegram or WhatsApp, have introduced end-to-end encryption in recent years has been convenient for terrorists and even incentivised moving their various online efforts, including recruitment, communication, and planning (cf. Gill et al. 2017) there. Such a development is commonly and hereafter referred to as the 'going dark' problem, as it increasingly places terrorists out of sight from intelligence services or criminal prosecution (West and Forcese 2020, 182; B. Kerr and Schneier 2018, 1019; Graham 2016, 20). This, in turn, impacts states' ability to protect national security. Crucially, the phenomenon has been observed across the ideological spectrum. Both al-Qaeda and Daesh have allegedly evaded state surveillance and

prosecution by using end-to-end encrypted communication, just like individual terrorists such as the Paris perpetrators who reportedly used encrypted messaging platforms for planning their attacks (Klausen 2015, 3; Graham 2016, 23). However, right-wing extremists have recently augmented authorities' concerns in particular, due to their significant online presence on end-to-end encrypted social media (cf. Baele, Brace, and Coan 2020), adding renewed urgency to governments' discontent over the shortcomings of states' traditional communications interception capabilities (McGarrity and Hardy 2020, 162).

2. The Investigatory-Capabilities Gap

Such concerns about what Hale-Ross (2018, 2) refers to as an 'investigatory-capabilities gap' appear justified in light of various reports quantifying the loss of intelligence due to increased end-to-end encryption of communication. Examples include Canada, where 70% of intercepted communications appeared in unreadable ciphertext in 2018 (West and Forcese 2020, 185) or Australia, where end-to-end encryption impeded up to 90% of high-profile terrorism investigations (McGarrity and Hardy 2020, 169). Consequently, security authorities face increasing pressure to close the investigatory-capabilities gap, seeking answers to the following key question: How can counterterrorism adapt to the 'going dark' phenomenon?

The range of options to solve this problem may be placed on a spectrum with two extremes (cf. Castro and McQuinn 2016). On one side lies authorities' option of capitulation in the form of refraining from communications interception on messaging platforms offering end-to-end encryption. This would keep everyone's communications, including those of terrorists, protected from the eyes of security authorities, while the latter could at most expand other ways of gathering information to compensate for the resulting loss of intelligence. On the other side of the spectrum are bans on end-to-end encryption as such or of a certain

strength. This political solution would re-enable communications interception in its traditional form while significantly weakening digital security systems.

The only available middle-ground for dealing with the 'going dark' problem is to utilise 'workarounds'. In the case of end-to-end encryption, where only the receiver can decrypt the message with their private key, this would mean finding ways 'to reveal a plaintext version of a target's data that has been concealed by encryption' (B. Kerr and Schneier 2018, 991) without the key. Such a strategy would make it possible to keep end-to-end encryption as a 'fundamental component of improving cybersecurity' (Castro and McQuinn 2016, 2) while enabling law enforcement and intelligence agencies to intercept individuals' virtual communications when necessary.

However, these workarounds also demonstrate that the 'going dark' problem is rather a Gordian knot whose only solution appears to require rather unconventional means. A fitting example is the so-called 'State Trojan', spyware installed onto the target person's end device, which intercepts their ongoing communication. Lawful telecommunications surveillance by state authorities to protect citizens from terrorist threats has historically always been controversial (Fitsanakis 2020), but the use of state spyware is repeatedly met with fierce resistance, especially from advocates of civil liberties. They perceive the State as an intruder who insidiously breaks into private communications and erroneously understands data protection to be the problem (Ronellenfitsch 2007, 568). Hence, the critical question for security authorities seeking to fill the 'investigatory-capabilities gap' is the following: How can counterterrorism efforts maintain a balance between security and individual liberties while using State Trojans?

This question will be examined in the German context in this paper, as there are two reasons why the developments in this country are particularly promising for discussion. On the one hand, the German parliament and security authorities explicitly justify using State

Trojans by pointing to the need of closing 'intelligence gaps' due to new challenges posed by end-to-end encryption (Bundestag 2021, 8). On the other hand, Germany is internationally known for its historical and ongoing affinity to data protection (Ronellenfitsch 2007, 562), as further evidenced by the creation of a fundamental IT-right, which is particularly endangered by the use of State Trojans.

In this paper, I first outline the changes to the domestic legal framework that enabled the use of spyware as a law enforcement tool and expanded such powers to German intelligence services. Subsequently, I discuss the proportionality of State Trojans with regard to their impact on fundamental rights focusing on three problematic issues: the anticipatory logic underlying their employment and rendering thresholds of use unclear, the technical difficulties for their controlled use and the necessary trade-offs concerning information technology (IT) infrastructure. Based on the profound evidentiary impact on fundamental rights, I argue that the spyware's use as a counterterrorism tool only strikes a fair balance between security and liberty if certain safeguards are put in place, which I outline in closing.

3. Interception Through Equipment Interference in Germany

Before discussing whether and how State Trojans may be problematised with regard to civil liberties, one must first understand how and why this spyware entered German counterterrorism practice. Until 2021, only the Federal Criminal Police Office (BKA) could monitor any telecommunications, ever since legislative changes in January 2008[1] authorised this law enforcement agency to monitor and record telecommunications without the target's knowledge to avert threats of international terrorism[2] (Federal Ministry of Justice 2017). Somewhat abstractly, these legal provisions specify that the interception of communications is lawful if the

[1] 'Gesetz zur Neuregelung der Telekommunikationsüberwachung' (Act on the Reorganisation of Telecommunications Surveillance).
[2] §§5, 51(2) Federal Criminal Police Office Act.

target is a person in respect of whom certain facts justify the assumption that they will commit a terrorist offence within a foreseeable period of time and in a manner that is at least concrete in terms of its nature (Ibid.). A subsequent legislative change[3] aiming at making criminal investigations more 'effective and practicable' (Deutscher Bundestag 2017, my translation) supplemented this legal framework by authorising a particular type of communications interception that introduced an equipment interference capability termed 'Quellen-TKÜ'.

This method differs from traditional lawful interception in that authorities interfere with the 'source' of the communication, the targeted person's end device and IT system (Freilich, Safferlin, and Rückert 2017). As a criminal procedural measure, such hacking-based interception is now covered under §100a (section 1, para. 2-3) of the Federal Criminal Police Office Act, which further states that 'telecommunications may also be intercepted and recorded in such a manner that technical means are used to interfere with the information technology systems used by the person concerned if this is necessary to enable interception and recording in unencrypted form in particular' (Federal Ministry of Justice 2017, official translation). Such 'technical means' refer to the use of specific spyware, the aforementioned 'State Trojan', which is secretly implanted, either through direct access to the device or through links, email attachments, software updates, or website re-directs to websites infected with the spyware. This method constitutes a strategy for overcoming surveillance difficulties with end-to-end encryption as a State Trojan's placement enables the interception of ongoing communication by forwarding it to the authorities before encryption or after decryption[4] (Federal Ministry of Justice 2017; Denning and Baugh 1999, 264).

[3] 'Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens' (Act on the more effective and practicable organisation of criminal proceedings).
[4] §51 para. 2 Federal Criminal Police Office Act.

A State Trojan's employment is thus, according to the German parliament, in the public interest since it constitutes a reaction to 'the changed communication habits involving the use of modern technology' (Bundestag 2021, 8, my translation). Furthermore, it is intended to close the existing 'intelligence gap' caused by end-to-end encryption and recover authorities' capabilities to protect against both far-right and Islamist terrorist threats. The same reasoning was applied to the subsequent expansion of the powers to use equipment interference for communications interception to intelligence agencies. In October 2020, the Federal Cabinet passed a bill, which entered into force on 9 July 2021[5], to amend legislative frameworks by enabling all German domestic intelligence services to conduct the 'Quellen-TKÜ' (Deutscher Bundestag 2021), constituting a significant widening of their competencies.

For all its powers, however, the use of source-based intelligence and thus the employment of State Trojans is subject to strict conditions. What the German Federal Ministry of the Interior describes as 'narrow conditions and strict procedures for independent order and implementation control' (2021, my translation) include, for example, making the deployment of such spyware subject to judicial order. Furthermore, its use for intelligence purposes requires further authorisation by the so-called G10 Commission, a parliamentary oversight body recently supplemented by a technical advisor. However, such protective measures should not distract from the fact that these changes to the domestic legal framework are nonetheless controversial and require critical scrutiny. In the following, I will embed the use of State Trojans in the nexus between national security and civil liberties and subsequently examine to what extent their balance may be at risk.

[5] 'Gesetz zur Anpassung des Verfassungsschutzrechts' (Law on the Amendment of the Law on the Protection of the Constitution).

4. A Balancing Act of Competing Social Goods

The 'perennial question about the balancing of security against freedom' (Richards 2016, 74) lies at the heart of counterterrorism - in the analogue as well as in the digital space. More specifically, one may understand citizens' right to state protection from threats to their life or the liberal democratic system on the one hand and individual liberties on the other hand as two competing social goods that all counterterrorism efforts must balance (Bellovin et al. 2014, 45; Denning and Baugh 1999, 274). This liberty-security nexus is not just a philosophical but also a practical balancing act since it is anchored in Germany's fundamental law, the Grundgesetz. According to the former president of the German Constitutional Court, the latter contains a mandate to defend against damage to the democratic order while observing the rule of law (Papier 2012). A particular obligation thereunder is the prohibition of unreasonable encroachments on citizens' fundamental rights, which thus represents a natural limit of the State's duty to protect (Ibid.).

How can such an obligation be reconciled with equipment interference using State Trojans that represent, according to some critics, 'perhaps one of the most intrusive powers available' (Hale-Ross 2018, 83)? From a legal perspective, one can differentiate between two constitutional barriers to the use of intrusive state measures for collective security: While core liberties such as human dignity merit absolute protection and may not be restricted by any measure, the restriction of other freedoms outside this category is subject to the principle of proportionality (Papier 2012). In this case, the legislator needs to deliberate whether an encroachment on these fundamental rights and its severity is necessary and proportionate in relation to the gained benefit of the measure (Ibid.). When these considerations are applied to the decision to interfere with an IT system using a State Trojan for communications surveillance, one conflicting right to freedom stands out in particular: Germany's fundamental right to the guarantee of the confidentiality and integrity of information technology systems,

hereafter fundamental IT right. This was derived by the German Federal Constitutional Court (2008) from the general right of personality[6] and is intended to protect citizens from unlawful interference with or manipulation of their information technology systems, including by the State. As current lawsuits before the German Federal Constitutional Court attest, it is above all this fundamental IT right that the use of state spyware may disproportionately curtail and makes one question whether the authorities' solution to the 'going dark' Gordian knot can strike a fair balance between liberty and security.

5. Three Problems with the State Trojan

As Castro and McQuinn (2016, 14) aptly state, each solution to fill the investigatory-capabilities gap caused by end-to-end encryption 'comes with trade-offs in the form of different levels of security risk and reliability of access for law enforcement and intelligence agencies'. By way of example, this paper will now outline three problematic areas that either render testing proportionality more difficult or cast doubt on its applicability outright. The discussion centres around three questions: When, to what extent, and with what trade-offs may State Trojans be used for counterterrorism purposes?

5.1 Inhibition Thresholds – Anticipatory or Pre-crime logic?

The first problem lies in the lack of clarity about the main purpose of the State's profound interference in individuals' IT systems and the intervention thresholds. By expanding the powers to use this method from law enforcement to intelligence agencies, the legislator has shifted authorities' focus forward to the preventative field, resulting in uncertainty about when individual civil liberties might be at risk or curtailed. On the one hand, it may be argued that equipment interference with State Trojans, therefore, exemplifies a 'fundamental

[6] Art. 2.1 in conjunction with Art. 1.1. of the Basic Law (Grundgesetz).

jurisprudential shift from [a] current ex post facto system of penalties and punishments to ex-ante preventative measures' (I. Kerr and Earle 2013, 66), or that the associated restriction of fundamental rights follows a 'pre-crime logic of security' shifting 'the temporal perspective to anticipate and forestall that which has not yet occurred and may never do so' (Zedner 2007, 262).

On the other hand, Hale-Ross (2018, 106) argues that such pre-crime terminology is purely fictional and that even preventative measures are post-criminal. This means that a State Trojan, for example, is a justified preventative hacking tool for targeting individuals that have already committed criminal offences, such as the formation of a terrorist organisation following §129a German Criminal Code (Federal Ministry of Justice 2021a), but that are expected to commit even more serious ones, such as a terrorist attack. Therefore, it would reflect an 'anticipatory risk management approach' (Hale-Ross 2018, 107) rather than a pre-crime logic.

However, this scholarly disagreement about what logic underlies the new communications interception measures rather underlines the uncertainty on intervention thresholds. According to the German authorities, a judicial order for a lawful interception with State Trojans is not contingent on an imminent danger or a criminal suspicion, which adds to concerns about the intervention threshold being subjectively placed in the run-up to suspicion. Consequently, decisions on whether to use state spyware and thus restrict individual civil liberties of the target, such as the fundamental IT right, have become dependent on risk prognoses. The fact that these are commonly based on probability calculations creates a possibility for miscalculations and risks that the grounds for intervention are consequently shifted too much into the run-up to a threat situation (Papier 2012). In combination with authorities' vague statements about the necessity of factual grounds of substantial dangers as a prerequisite for an IT system interference in the context of communications surveillance, this results in the

impression of leaving too much room for interpretation for decision-makers to carry out a meaningful proportionality test. Furthermore, it induces a lack of trust in the same authorities to make the right operational decisions and makes regular users of end-to-end encrypted platforms wonder whether their personal freedoms in the digital space, which they expect to be protected under the fundamental IT right, might be erroneously at risk.

5.2 Technical Dilemmas

Another problem arises with regard to the technical feasibility of State hacking through the use of State Trojans. First, since it is hitherto unclear how to control that such spyware, once placed in the system under investigation, does not extract more data than expressly instructed (Bellovin et al. 2014, 48; Ronellenfitsch 2007, 568), a proportionality test when deciding on the use of lawful state hacking is only possible based on anticipations about the scope of interference with fundamental rights. Meanwhile, German legal scholars deny that a reliable mechanism to sufficiently control the scope of an interference with an individual's IT system for counterterrorism purposes exists (cf. Stadler 2012; Buermeyer 2013). Consequently, a final proportionality test is only possible ex post facto, and these what have been already called 'technical dilemmas' (West and Forcese 2020, 198) thus reinforce the risk of disproportionate encroachments of civil liberties.

Furthermore, while until the mid-1990s, most telecommunication services were state-run, lawful interception nowadays necessarily involves the assistance of private actors in a twofold manner: First, mobile phone companies, internet providers, or commercial WLAN operators are to assist in the placement of a State Trojan upon authorities' request (Deutscher Bundestag 2020, 7; McGarrity and Hardy 2020, 170). Second, law enforcement and intelligence agencies use not only their own proprietary spyware but also one purchased from a private German-British company. This raises both moral and practical questions about the extent to which the German State can and should oblige private companies to actively

assist in equipment interference and whether the consequences thereof are proportionate to the gain in intelligence or criminal evidence. Private companies are known for their reluctance to break data privacy commitments to their customers, partly due to their underlying convictions and partly for competitive reasons (B. Kerr and Schneier 2018, 1016; Bellovin et al. 2014, 49). Furthermore, the extent of financial and reputational effects of obligatory technical assistance with the employment of spyware in communications interception remains an open question (McGarrity and Hardy 2020, 180). Finally, a key ethical concern is the potential risk that some companies may exploit the security authorities' dependence on their expertise and misuse it for other purposes. Here, too, the consequences are not foreseeable, and questions about liability remain unanswered.

5.3 Collateral Damage to IT Infrastructures

The final problem area shifts the question of proportionality away from looking at the infringement on an individual's civil liberties to the secondary effects of equipment interference on all citizens' fundamental freedoms. First, the previous problems may result in a general loss of trust in law enforcement and intelligence agencies' decision-making. The anticipatory approach of hacking-based interception and the associated risks of misjudgement and subjectivity may contribute to an overall societal uncertainty and loss of trust in law enforcement and intelligence agencies and thereby potentially delegitimise counterterrorism efforts in general. Similarly, trust in network operators and private companies, which for the first time are transformed from passive actors into active accomplices of the security authorities, may be undermined with adverse economic consequences.

Apart from these concerns, a widespread criticism of state spyware is that its employment necessitates weakening wider IT infrastructures. A State Trojan can only be secretly installed on the target's end device by deliberately exploiting security vulnerabilities in their IT infrastructure or encryption code. Many critics of the legislative changes thus fear

that the prospect of overcoming the investigatory-capability gap may create incentives for authorities to develop or leave such 'backdoors' open to allow later or regular exploitation (B. Kerr and Schneier 2018, 1006) instead of closing them for improved general data security (Hale-Ross 2018, 86; Bellovin et al. 2014, 49). Even if they do not actively place vulnerabilities in the system, 'law enforcement's inactivity is potentially enabling criminal exploitation of vulnerabilities to the detriment of all users of the respective hardware or software' (Ibid., 46).

Hence, the dilemma is that while the State Trojan's purpose is to enable law enforcement and intelligence agencies to protect society from terrorist threats, the spyware's deployment requires at least the maintenance of severe security risks for the national IT infrastructure while the public relies on the State to protect the confidentiality and integrity of their IT systems. A first of several constitutional challenges against the changes in the German legal framework allowing state hacking techniques, arguing that the State disregards its duty to protect citizens' digital security by keeping IT vulnerabilities secret (Zillekens 2021), was recently dismissed. Nevertheless, the Federal Constitutional Court (2021) also acknowledged the existence of a trade-off between the protection of IT systems against criminals exploiting vulnerabilities and the State's duty to protect public safety through lawful interception, for which it has become necessary to keep such vulnerabilities open. However, is it also proportionate to endanger the right of all citizens to secure IT infrastructures based on suspicions and anticipations, as is characteristic of counterterrorism efforts?

As a combination of the two, a final risk is the increasing self-infliction of vulnerability resulting from a lack of trust in authorities' decision-making and discretion. Even unwarranted concerns that software updates may install vulnerabilities and backdoors to facilitate authorities' equipment interference for communications surveillance may 'discourage

consumers from patching security vulnerabilities on their devices' (Castro and McQuinn 2016, 18).

4. Problematic but not Uncompromising Decisions

As a workaround for end-to-end encrypted telecommunications, the use of State Trojans is intended to close the investigatory-capabilities gap of law enforcement and intelligence agencies in the fight against terrorism and thus protect citizens from terrorist activities and attacks. At the same time, equipment interference conflicts with fundamental rights - primarily the fundamental right of citizens to the confidentiality and integrity of information technology systems. This is a freedom that is not absolute but whose restriction requires a proportionality test. However, the aforementioned three problem areas illustrate that it can be challenging to assess whether the so-called 'Quellen-TKÜ', a method of lawful state hacking, unsettles the balancing act between the conflicting social goods of IT rights and collective security.

Firstly, it is unclear to what extent individual liberties are threatened since the logic behind equipment interference for interception is, at least since the extension of powers to intelligence agencies, an anticipatory one and the threshold of use moves further and further into the area of suspicion. As a result, it remains ambiguous who can become the target of such state hacking and at what time. The uncertainty following this is exacerbated by the lack of technical ability to sufficiently control the scope of information gathering. Most serious, however, is the fact that communications surveillance through equipment interference requires the exploitation of vulnerabilities in IT infrastructures and thus endangers the digital security of all internet users, which arguably constitutes an indirect breach of the fundamental IT right in itself.

Such ambiguities make it difficult to answer the principal question: Does the communications interception through equipment interference cause more damage by violating the

fundamental IT right than it may protect national security from terrorism? Put differently, are State Trojans and their consequences a lesser evil to protect against the greater evil of terrorism or is it the other way round?

However, such questions may overestimate the actual frequency of communications interception through equipment interference. They may further mistakenly suggest an either-or-question that does not reflect reality since communications surveillance is only one component of a larger and complex set of counterterrorism efforts. Thus, before rejecting state hacking as a solution for the 'going dark' problem outright, due to this abeyance of constitutional and moral questions, it is useful to put the discussion in relation to its actual application. For the first time, the annually published statistics on communication surveillance in the reporting year 2019 also contained data on equipment interference. Out of 31 court-ordered interferences with an IT system, only three were ultimately carried out (Federal Ministry of Justice 2021b). Firstly, such evidence of its sparse use serves as a reminder that infiltrating individuals' IT systems with state spyware is a complex and elaborate process, requiring technical expertise and financial resources (Hale-Ross 2018, 84). Secondly, it may suggest that the prerequisites of judicial and parliamentary orders are fairly high bars in practice. When taking these relativising aspects into account, the use of State Trojans may still be considered problematic but re-negotiable.

Furthermore, if Bellovin et al.'s (2014, 64) suggestion that only 'vulnerabilities already present in the target's communication device' are exploited was a prerequisite for equipment interference, the risk posed by leaving vulnerabilities secret and unpatched might be present, yet manageable. After all, private companies are continually searching for IT vulnerabilities to protect their customers, while the State seems to make only scarce use of State Trojans. Yet, this reasoning underlies the assumption that this will continue to be the case and has the consequence that the responsibility for protecting the integrity of IT systems and

security of digital infrastructures increasingly shifts to private actors. Nevertheless, these two attenuating additions suggest that the 'going dark' problem does not necessarily present security agencies with a choice of two evils, namely surrendering complete data protection or accepting their inability to monitor terrorist communications. Instead, it suggests that engaging in a balancing act of collective security and individual liberties may not be impossible.

6. Conclusion and Outlook

If the previous examination has shown one thing, it is that the 'going dark' problem's description as 'one of the most difficult policy dilemmas of the digital age' (Castro and McQuinn 2016, 1) is warranted. The question of whether insight into end-to-end encrypted terrorist communications or the continuous protection of the IT security of the entire population weighs more is a matter of discretion. Furthermore, it underlines the tension between security and civil liberties inherent in all counterterrorism efforts. If law enforcement and intelligence agencies are not willing to acquiesce to the investigatory-capabilities gap, they currently seem to have no other choice but to use state spyware and exploit system vulnerabilities. On the one hand, 'there is no technological solution to square this circle' and on the other, 'there is simply no way to ensure that third-party access by a company or government actor is not also abused by adversaries' (Castro and McQuinn 2016, 29).

However, if we consider that the software is likely to be used infrequently and assume that the State is only exploiting existing vulnerabilities and not creating them itself, we can focus on the question of how the State could proactively ensure that the balance between different social goods is maintained (cf. Herpig 2018). If law enforcement and intelligence agencies nevertheless want to retain communications interception through equipment interference, they can at least address the difficulties problematised in this paper.

There is especially potential for improvement in the communication and precision of the legal provisions and rules on using State Trojans. The problem areas sketched out in this paper suggest that the scope and thresholds of intervention (Hale-Ross 2018, 8) of state hacking must first be clearly defined. This may be realised by establishing rules on intervention thresholds based on suspicion or danger levels (Papier 2012) and holding decision-makers accountable for compliance with them. Furthermore, it must be ensured that the State Trojan constitutes a 'trustworthy and reliable' (Bellovin et al. 2014, 48) instrument that does not inadvertently, fraudulently, or excessively collect data (Hale-Ross 2018, 8).

On the one hand, this includes technical due diligence, which could be exercised, for example, through technical certification and regular mandatory inspection and improvement of the spyware. Furthermore, it must also be ensured that if too much data is intercepted and collected, it is immediately and irrevocably deleted (Papier 2012; Bellovin et al. 2014, 64). On the other hand, this calls for independent control of State Trojans' deployment and accountability to the public so that the trust in the State's protective role against terrorism is augmented rather than damaged.

Despite all these safeguards, a residual risk for IT infrastructures and thus the digital security of the population is inherent in the use of state surveillance software. For this reason, too, the future use of these state hacking techniques should be subject to continuous evaluation and made dependent on whether such measures are expedient (B. Kerr and Schneier 2018, 992).

7. Reference List

Baele, Stephane J., Lewys Brace, and Travis G. Coan. 2020. 'Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda.' *Studies in Conflict & Terrorism*. https://doi.org/10.1080/1057610X.2020.1862895.

Bellovin, Steven M., Matt Blaze, Sandy Clark, and Susan Landau. 2014. 'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet.' *Northwestern Journal of Technology and Intellectual Property* 12 (1–2): 1–66.

Buermeyer, Ulf. 2013. 'Zum Begriff der "laufenden Kommunikation" bei der Quellen-Telekommunikationsüberwachung.' *Strafverteidiger* 470.

Bundestag. 2021. 'Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikations- Überwachung durch Nachrichtendienste.' Wissenschaftlichen Dienste des Deutschen Bundestages. https://www.bundestag.de/resource/blob/830002/3a1ed4b31d92b8575b3f31e496128d8f/WD-3-293-20-pdf-data.pdf.

Castro, Daniel, and Alan McQuinn. 2016. 'Unlocking Encryption: Information Security and the Rule of Law.' Information Technology & Innovation Foundation. March 14, 2016. https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law.

Denning, Dorothy E., and William E. Baugh. 1999. 'Hiding Crimes in Cyberspace.' *Information, Communication & Society* 2 (3): 251–76. https://doi.org/10.1080/136911899359583.

Deutscher Bundestag. 2017. 'Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens.' Deutscher Bundestag. August 17, 2017. http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3202.pdf.

———. 2020. ‘Sachstand: Maßnahmen gegen Gefährder.’ Deutscher Bundestag. November 19, 2020. https://www.bundestag.de/resource/blob/817826/34cb38786cf02bef95a4c34b59c43f89/WD-3-260-20-pdf-data.pdf.

———. 2021. ‘Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts der Bundesregierung.’ Deutscher Bundestag. February 19, 2021. https://www.bundestag.de/resource/blob/830002/3a1ed4b31d92b8575b3f31e496128d8f/WD-3-293-20-pdf-data.pdf.

Federal Constitutional Court. 2021. ‘Constitutional Complaint Regarding the Police’s Handling of Security Vulnerabilities in IT Systems Is Inadmissible.’ Press Release No. 62/2021. June 8, 2021. https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2021/bvg21-062.html.

Federal Ministry of Justice. 2017. ‘Federal Criminal Police Office Act.’ Bundesjustizministerium. https://www.bka.de/DE/DasBKA/GesetzlicherAuftrag/gesetzlicherauftrag_node.html#doc20666bodyText1.

———. 2021a. ‘Strafgesetzbuch (StGB)’. Bundesjustizministerium. https://www.gesetze-im-internet.de/stgb/__129a.html.

———. 2021b. ‘Übersicht Telekommunikationsüberwachung für 2019.’ Bundesjustizministerium. https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html.

Federal Ministry of the Interior. 2021. ‘Fragen und Antworten zum Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts.’ Häufig nachgefragt.

https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/sicherheit/anpassung-verfassungssschutzrecht/faq-liste-anpassung-verfassungsschutzrecht.html.

Fitsanakis, Joseph. 2020. *Redesigning Wiretapping: The Digitization of Communications Interception*. History of Information Security. Cham: Springer. https://doi-org/10.1007/978-3-030-39919-1.

Freilich, Felix, Christoph Safferlin, and Christian Rückert. 2017. 'Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen.' *Juristische Rundschau* 2018 (1): 9–22. https://doi.org/10.1515/juru-2017-0104.

German Federal Constitutional Court. 2008. Judgement of the First Senate of 27 February 2008. 1 BvR 370/07. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.

Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. 2017. 'Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes.' *Criminology & Public Policy* 16 (1): 99–117. https://doi.org/10.1111/1745-9133.12249.

Graham, Robert. 2016. 'How Terrorists Use Encryption.' *CTC Sentinel* 9 (6): 20–25. https://ctc.usma.edu/how-terrorists-use-encryption/.

Hale-Ross, Simon. 2018. *Digital Privacy, Terrorism and Law Enforcement: The UK's Response to Terrorist Communication*. London: Routledge. https://doi.org/10.4324/9781351118989.

Herpig, Sven. 2018. 'A Framework for Government Hacking in Criminal Investigations.' Berlin: Stiftung Neue Verantwortung e.V. https://www.stiftung-nv.de/sites/default/files/a_framework_for_government_hacking_in_criminal_investigations.pdf.

Kerr, Bruce, and Bruce Schneier. 2018. ‘Encryption Workarounds.’ *Georgetown Law Journal* 106 (4): 989–1020.

Kerr, Ian, and Jessica Earle. 2013. ‘Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy.’ *Stanford Law Review Online* 65: 56–72. https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_Stan-LRevOnline_65_KerrEarle.pdf.

Klausen, Jytte. 2015. ‘Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq.’ *Studies in Conflict & Terrorism* 38 (1): 1–22. https://doi.org/10.1080/1057610X.2014.974948.

McGarrity, Nicola, and Keiran Hardy. 2020. ‘Digital Surveillance and Access to Encrypted Communications in Australia.’ *Common Law World Review* 49 (3–4): 160–81. https://doi.org/10.1177/1473779520902478.

Papier, Hans-Jürgen. 2012. ‘Das Bundesverfassungsgericht Und Die Innere Sicherheit.’ In *10 Jahre 11. September - Die Rechtsordnung im Zeitalter des Ungewissen*, edited by Kyrill-Alexander Schwarz, 27–40. Baden-Baden: Nomos Verlagsgesellschaft. https://doi.org/10.5771/9783845237565-27.

Richards, Julian. 2016. ‘Needles in Haystacks: Law, Capability, Ethics, and Proportionality in Big Data Intelligence-Gathering.’ In *Big Data Challenges: Society, Security, Innovation and Ethics*, edited by Anno Bunnik, Anthony Cawley, Michael Mulqueen, and Andrej Zwitter, 73–84. London: Palgrave Macmillan. https://doi.org/10.1057/978-1-349-94885-7.

Ronellenfitsch, Michael. 2007. ‘Datenschutzrechtliche Schranken bei der Terrorismusbekämpfung.’ *Datenschutz und Datensicherheit* 31 (8): 561–70.

Stadler, Thomas. 2012. ‘Zulässigkeit der heimlichen Installation von Überwachungssoftware.’ *MultiMedia und Recht* 18.

West, Leah, and Craig Forcese. 2020. ‘Twisted into Knots: Canada’s Challenges in Lawful Access to Encrypted Communications.’ *Common Law World Review* 49 (3–4): 182–98. https://doi.org/ 10.1177/1473779519891597.

Zedner, Lucia. 2007. ‘Pre-Crime and Post-Criminology?’ *Theoretical Criminology* 11 (2): 261–81. https://doi.org/10.1177/1362480607075851.

Zillekens, Janina. 2021. ‘Wir klagen gegen Staatstrojaner.’ Gesellschaft Für Freiheitsrechte. June 10, 2021. https://freiheitsrechte.org/staatstrojaner-faelle/.