CSR Cyber Security Raad

Visiting address
Turfmarkt 147
2511 DP The Hague

Postal address
PO Box 20011
2500 EA The Hague

I www.cybersecurityraad.nl
T +31 (0)70 751 5333 (secretariat)
E info@cybersecurityraad.nl

Ministry of Justice and Security
Attn: Ms D. Yeşilgöz-Zegerius
PO Box 20301
2500 EH The Hague

Date
23 August 2022

Subject
Advisory document regarding realistic alternatives for gaining lawful access to end-to-end encrypted communication, other than weakening encryption

Your Excellency,

The availability and usage of end-to-end encryption[1] has drastically increased in recent years. By implementing this form of encryption, electronic messaging services such as WhatsApp, Signal and Telegram demonstrate their strong commitment to protecting the privacy of users and to guaranteeing the confidentiality of their communications. This is a good thing, yet as is so often the case in the complex digital realm, this too has a dark side: strong encryption hampers the ability of intelligence and investigative services to do their jobs, allowing other safety risks (in the broad sense) to emerge. The use of such encryption is impacting criminal investigations, which are becoming increasingly complex[2] due to the opportunities digitalisation unfortunately offers to criminals as well. This is evident in the growth of cyber and digital crime.

The problems in connection with maintaining the ability of intelligence and investigative services to lawfully access the communications (including secure communications) and digitally stored information of suspects or victims have your attention at this time. Various national and/or scientific studies and inventories in relation to this topic are currently being conducted. As a result, it will be possible to compile arguments pertaining to various themes and issues for the purpose of conducting a well-informed public discourse and taking policy decisions. The Cyber Security Council (hereinafter: the CSR) applauds these initiatives.

The European Union similarly views the development of strong encryption for electronic communication as a precondition for ensuring the fundamental rights of citizens and their digital security on the one hand, while on the other it is necessary that the authorised investigative and intelligence services continue to be able to adequately perform their duties both online and offline. This presents us with a new dilemma concerning encryption, for which no solutions that can fully satisfy all the various interests are expected to be forthcoming in either the short or medium term.

The CSR therefore urges that – in anticipation of the aforementioned discussions and investigations and without taking a position as to whether or not functional or technical curtailment of encryption is desirable – an effort be made to explore the realistic alternative possibilities that are necessary for the performance of intelligence and investigative tasks. The government, after all, has an obligation of effort towards its citizens when it comes to realising social safety and order.

[1] End-to-end encryption ensures that only the sender and recipient can read or listen to the information in question.
[2] See for instance Policing in a changing environment | Working Paper | WRR

CSR Cyber Security Raad

In this letter, the CSR offers advice on realistic alternatives for gaining lawful access to end-to-end encrypted communication, other than weakening encryption. In doing so, the CSR wishes to emphasise that while the alternatives in question are not likely to yield a full-fledged replacement, it is nevertheless the opinion of the Council that a broad, different approach to this issue is *both valuable and necessary*.

Background

Traditional telephone services involve central hubs controlled by private or national telecom providers, where the relevant communications are available and where taps may be installed, subject to national jurisdiction. The commercially available telecom infrastructure was designed with this in mind and therefore includes standardised technical, legal and organisational interception functionalities. That being said, modern electronic communication services operate over the internet, frequently beyond the purview of telecom providers, meaning there are no fixed tap points. Such over-the-top (OTT) services are making increasingly frequent use of end-to-end encryption. As a result, the interception methods usually applied to these OTT services are no longer effective and a great deal of substantive communication has become inaccessible.

It is not only lawful access to encrypted communication via OTT services that is under pressure: the 5G telecom infrastructure currently being rolled out requires adjustments as well. Potential solutions to this problem are being explored at this time. The encryption of signal information in the 5G network means that a foreign 5G smartphone cannot, in principle, be tapped in the Netherlands and vice versa. Here, too, there is talk of maintaining the current possibilities in order to allow for and preserve the possibility of national tapping of international telephones.

Arriving at solutions for the OTT-related interception problems described will require a joint European approach: we are, after all, dealing with globally operating providers. This also applies to 5G solutions, which call for new international agreements between telecom providers and governments with regard to lawful access, in terms of both technical standards and the harmonisation of legislation.

Exploring alternatives for lawful access by intelligence and investigative services

The CSR has conducted a brief inventory study aimed at alternatives to the curtailment of encryption. The Council has done so primarily from a technical perspective, making use of the recommendations and overview submitted by a technical task force. Two areas appear to offer promising starting points, namely (A) the optimisation of hacking activities, and (B) making more intensive use of operational data (hereafter: operational logs). In the appendix[3] to this letter, you will find the report from the aforementioned technical task force, which provides a more detailed explanation of both areas. Based on this report, the CSR has drawn the following conclusions:

A. *Optimisation of hacking activities*

It is the conclusion of the CSR that, while it is true that hacking is a highly valuable instrument for intelligence and investigative services, in terms of scalability and predictability of the output, it cannot compare to tapping regular telephone service by means of cooperation from the providers of public telecommunications networks and services – cooperation such providers are obligated to provide under the Telecommunications Act. The practical deployability of the hacking powers could be improved by means of more suitable legal frameworks and supervision, in combination with technical optimisation. Embedding and streamlining hacking as an investigative tool will make it possible to deploy this approach more quickly and more efficiently, thereby reducing impediments to its use.

B. *Making more intensive use of operational logs*

The CSR concludes that there is still much progress to be made in this regard; businesses are currently often very slow to comply, or provide only partial compliance, with their legal duty to turn over operational logs in

[3] Final report from the technical-substantive task force on realistic alternatives for encryption, The Hague, 25 March 2022

response to statutory requests from government bodies in the realm of investigation and security. Firstly, it is possible to operate in a more assertive fashion within the current frameworks and, by doing so, to create case law – thereby increasing the specificity and predictability of such procedures. Secondly, new legislative processes, including those aimed at strengthening the statutory basis for national and international data requests, can further eliminate obstacles and ambiguities and promote more effective cooperation and better-defined frameworks.

Recommendations

As a possible alternative for obtaining lawful access to encrypted electronic communication, the CSR recommends investing in the optimisation of hacking activities and making more intensive use of operational logs. This can be achieved by following up on the recommendations of the technical task force. However, because the alternatives in question will not yield a full-fledged replacement for the existing interception powers, the loss of tappability will continue to be felt.

The expectation is that it will be possible to adequately follow up on these recommendations, thanks in part to harmonisation and interpretation of legislation at the European level. To that end, European bodies for standardisation must be deployed, with joint ministerial responsibility within the Netherlands. The Ministry of Economic Affairs and Climate Policy could monitor the progress, for instance, while experts from the intelligence and investigative services could provide substantive contributions under the guidance of the Ministries of Justice and Security, Interior and Kingdom Relations and Defence.

The various recommendations are summed up below.

General joint recommendations to the Minister of Justice and Security and the Minister of Economic Affairs and Climate Policy:

1. *Rather than attempting to compensate for the reduced phone tap possibilities by means of a single measure, take a wider view of the matter by considering a spectrum of possible alternative approaches.*
2. *With regard to tapping 5G connections, implementation at the European level calls for the same transparency, uniformity and legal certainty which are now prevalent in the telecom industry.*

Joint recommendation to the Minister of Justice and Security and the Minister of Economic Affairs and Climate Policy regarding the intensification of hacking activities:

3. *Investigate the possibility of transparent legal regulations for enhanced access to telecom providers for the purpose of securing a better starting position for being able to hack specific smartphones.*

Recommendation to the Minister of Justice and Security regarding the intensification of hacking activities:

4. *Ensure more suitable legal frameworks and supervision, in combination with technical optimisation, in order to embed and streamline hacking as an investigative tool used by the police. It should also be noted that there are significant impediments to the use of hacking, that it is difficult to scale up, requires situation-specific action, is suitable primarily for major cases and is not guaranteed to yield the desired output.*

Joint recommendation to the Minister of Justice and Security and the Minister of Economic Affairs and Climate Policy regarding the use of operational logs:

5. *Compel online service providers to cooperate more effectively with the intelligence and investigative services with regard to the handover of operational logs. Eliminate any obstacles and ambiguities by, on the one hand, investing in closer cooperation and coordination and, on the other, parallel to these efforts, by making better use of the existing judicial possibilities for achieving timely handover. This can be achieved in the near term via case law and in the longer term via national and international legislation.*
6. *Approach these requests for information from a more Dutch/European perspective in order to avoid issues of interpretation under American law. Whenever possible, requests should be directed to the Dutch/European branch offices of the companies in question and should be conducted under European laws and regulations.*
7. *Invest more heavily in public-private partnerships with companies that provide services in the information society and emphasise the duty of care owed to society by large ICT companies.*

These recommendations have been submitted in writing to the Minister of Economic Affairs and Climate Policy as well. For information purposes, a copy of the recommendations has also been sent to:

- The Minister of Kingdom Relations and Digitalisation at the Ministry of the Interior and Kingdom Relations;
- The Minister of the Interior and Kingdom Relations;
- The Minister of Defence.

On behalf of the Cyber Security Council,

Sylvia van Es
CSR co-chair

Appendix: Final report of findings by the technical-substantive task force on encryption