SWP Comments

Stiftung
Wissenschaft und
Politik

German Institute
for International and
Security Affairs

Encryption under Threat

As states across the globe weaken cyber-security, Germany should oppose the trend

Matthias Schulze

An inadvertent worldwide alliance against encryption is emerging, as Western democracies join authoritarian regimes in weakening communication encryption and exploiting spyware. This accelerating global trend undermines efforts to enhance cyber-security. Germany should oppose such developments and intensify its efforts to champion encryption. This will also mean finding alternative instruments to keep terrorism suspects under surveillance without degrading the software security of the entire population.

Encryption technologies are a double-edged sword. On the one hand, encryption plays a vital role in the digital age, for example in online banking (SSL/TLS), secure web surfing (HTTPS) and the handling of sensitive data. It offers substantial protections against cyber-crime and hostile intelligence services. On the other hand, criminals can also use encryption to communicate beyond the reach of law enforcement. That dilemma forms the heart of a political debate that has continued for more than two decades. In the 1990s Washington considered banning encryption and requiring processor chips to be fitted with a backdoor permitting US authorities to eavesdrop encrypted communications ("Crypto Wars"). In the end, civil society resistance – together with technical obstacles – produced a broad consensus that more encryption made the digital world a safer place.

That consensus now appears to be crumbling. Whether driven by fear of terrorism or a wish to enforce censorship, more and more states are seeking ways to bypass encryption, for example by exploiting software vulnerabilities. As democratic states begin following authoritarian regimes down that road, there is a risk of this becoming the new international norm. Germany should oppose this trend, as software vulnerabilities endanger cyber-security for the population at large and encourage abuse, while the gains for counter-terrorism are limited.

China and Russia

In January 2017 Beijing introduced a federal licence requirement for Virtual Private Network (VPN) software. About 90 million Chinese use VPN clients to encrypt their entire internet communication – and evade

Matthias Schulze is an Associate in SWP's International Security Division

their government's internet surveillance and censorship infrastructure (the "Great Firewall"). Existing VPNs also allow users to access uncensored Western sources such as Wikipedia. State-licensed VPN services, however, would include the very surveillance and censorship filters that users are seeking to avoid. The new policy includes heavy fines for violations. Western companies operating in China have recently been required to switch to Chinese VPNs. Bowing to Chinese pressure, Apple has removed Western VPN clients from its Chinese iOS App Store.

Similar initiatives to bring VPN clients under state control exist in in Iran, Syria and most recently in Russia. The Russian Duma passed legislation in July 2017 forbidding the use of the Tor anonymisation network and VPN clients that fail to implement state censorship and internet surveillance (SORM-II). A year earlier, in July 2016, Russia adopted anti-terror legislation with provisions including expanded data retention and an obligation to grant the state backdoor access to encrypted services. This forces operators like Telegram and WhatsApp to hand encryption keys to the Russian authorities or to provide alternative access to their encrypted content.

United Kingdom, Australia, United States

The imposition of such drastic measures is not confined to authoritarian regimes. The British Investigatory Powers Act of 2016 contains provisions for state-mandated encryption and requires UK-based internet service providers to remove encryption on request. Companies can also be forced to create backdoors to give state agencies clandestine access, install eavesdropping software on their customers' equipment or block security updates. It is, however, unclear how London intends to make foreign companies comply with these requirements, which is why the measures have not yet been implemented. Undeterred by such difficulties, Australia is currently planning very similar legislation. The latest draft would allow law enforcement to force WhatsApp and other providers to provide access to encrypted communications.

In the United States the – as yet unenacted – Burr-Feinstein Encryption Bill of 2016 would require companies to deliberately weaken the (cyber)security of their products in order to make it easier for the authorities to access encrypted communications. Companies could also be compelled by court order to decrypt data for the authorities. The bill fulfils the FBI's demand to weaken the security mechanisms in the Apple iOS operating system, after it failed to access the encrypted iPhone of the 2016 San Bernardino attacker.

All these efforts must be seen in the context of an initiative by the "Five Eyes" intelligence alliance (United States, Canada, United Kingdom, Australia and New Zealand). Their objective is to establish a global regime that excludes terrorists from using encrypted communication. Given that this initiative aligns with Chinese and Russian interests, it advances a global norm-setting process in cyberspace. A Five Eyes communiqué of June 2017 proposes joint measures to enable legal access to encrypted communications. Although they say they want to cooperate with the IT industry, the states concerned are ignoring practical problems. In the past companies like Apple, Google and Microsoft have repeatedly resisted efforts to deliberately weaken their products.

Germany

Germany's position is contradictory. Berlin's cyber-security strategy of 2016 emphasises the benefits of encryption in areas such as digital public services and e-commerce ("security through encryption"), but also points to the dangers ("security despite encryption"). The Digital Agenda of 2014 even talks of making Germany the global leader in encryption. Agencies like the Federal Office for Information Security have long been warning of the dangers posed by

state backdoors and weakening encryption for law enforcement purposes.

However there are now signs of Germany walking back its strong cyber-security line. One indication is the new policing legislation of June 2017, which permits the use of surveillance software on devices like smartphones, another the founding of a dedicated agency to develop the requisite IT tools (ZITiS). In this approach the encryption software remains untouched, and instead the state spyware eavesdrops communication *before* it is encrypted on the device.

National security versus cyber-security

Hacking smartphones comes at a cost. It touches not only on questions of the right to privacy, which is protected under Article 10 of the German Basic Law, and the right to confidentiality of information systems formulated by the German Constitutional Court in 2008, but also erodes the overall standard of cyber-security.

Consensus exists within the global IT community that it is technically impossible to provide exclusive access for law enforcement without weakening the overall security of products. With current encryption procedures only authorised users (sender and recipient) can decrypt messages, and not third parties (hackers, authorities). So encryption not only ensures that the communication can be neither eavesdropped nor manipulated in transit (confidentiality and integrity), but also that the communication partners are actually those they appear to be (authenticity). The latest methods use session keys ("forward secrecy") or keys generated on a secure chip within the customer's device to make it technically impossible for the ISP to hand keys to the authorities or decrypt client communication themselves.

In such cases it is technically possible to monitor communication only before encryption. The required hacking or the use of special malware/spyware, depend in turn on software vulnerabilities to weaken or bypass the device's security mechanisms. But deliberately created or tolerated vulnerabilities will also be exploited by cyber-criminals and hostile intelligence services.

That is the dilemma: Either we weaken cyber-security in order to monitor terrorism suspects, and increase the risk of hacking and data theft. Or we accept the risk that certain criminals will no longer be so easy to keep under surveillance. Hacking and cyber-crime cause immense harm, estimated at up to $500 billion annually. That is what led James Clapper, former United States Director of National Intelligence, to insist that cyber-security – rather than terrorism – is now the leading national security threat.

So the costs of weakening software security are high, while the benefits tend to be small. Terrorists generally avoid services that are open to state eavesdropping. Once a service is known to have been compromised (like Skype since 2008), they switch to other channels. Besides "burner" phones and smartphones with multiple SIM cards (to run multiple WhatsApp and Telegram accounts), the Islamic State recommends using leave-no-trace operating systems like Tails to defend against spyware. The likely outcome of mandated vulnerabilities in smartphone software is that criminals will switch to other, more secure technologies while the general public's smartphones remain deliberately insecure. That would be reckless in light of the rise in cyber-security incidents and the growing numbers of affected users. The recent WannaCry ransomware attack affected hundreds of thousands of computers worldwide, while in Mexico Pegasus spyware was discovered on the smartphones of numerous journalists, lawyers and activists.

Recent developments like the Internet of Things and the trend to mobile working are changing the role of the smartphone, as they take on growing everyday control functions: Today, aside from communication, they administer bank accounts and digital wallets, open electronic locks and play a crucial part in cyber-security, for

example for two-factor authentication of online services. Compromising smartphones with spyware that can potentially be exploited by hackers and intelligence services undermines the security of all the associated services. And then there is the problem of the message this sends: If liberal democracies weaken software and encryption to fight terrorism, this will legitimise similar practices in authoritarian states.

Solutions

In light of the global initiatives by intelligence services and repressive regimes, Germany should advocate even more determinedly for secure software and encryption. At the same time alliances with other democratic EU states need to be strengthened, in order to stem the global trend against encryption. And instead of state-mandated software vulnerabilities undermining broader efforts to improve cyber-security, research needs to be put into developing new investigatory technologies and strategies.

An independent commission should assess how serious the problem of uncrackable encryption actually is. Calls for greater powers for the state are generally based only on anecdotal evidence, and there is in fact little in the way of reliable data concerning the number of investigations dropped on account of an inability to eavesdrop smartphone communication. Moreover, even in the known cases it is also often unclear whether alternative channels for accessing communication data might not have been available.

Such a commission could also take up the issue of developing new policing strategies. Since 2001 states have concentrated on technical surveillance capacities while in many cases steadily cutting back on staff. The extent to which more labour-intensive methods would be legal and useful needs to be considered. Cyber-crime investigations in the darknet are a good example. Illegal anonymous markets like Hansa and AlphaBay have been successfully closed down after their operators made mistakes or investigators set up sophisticated traps to harvest passwords and personal data. In the case of Hansa it was a property search that allowed investigators to gain access to the administrator's encrypted laptop. Alternatively, smartphone PINs could be acquired visually as they are entered. Such methods would grant the state legitimate access to encrypted communication by criminals without reducing cyber-security for the population as a whole.

SWP
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Telephone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1861-1761

Translation by Meredith Dale

(English version of SWP-Aktuell 56/2017)