SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

THE DEVELOPMENT OF ELECTRONIC SURVEILLANCE NORMS IN THE NETHERLANDS

Peter Koop

ABOUT THE AUTHOR

Peter Koop studied law in Amsterdam and from a lifelong interest in signals intelligence, cryptography and communications security, he became an independent researcher sharing his findings on the weblog Electrospaces.net, in various other publications and through lectures. He is one of the few people in the world who systematically and critically studied the documents from the Snowden revelations. Koop is a member of the Netherlands Intelligence Studies Association (NISA) and he participated, as a recognized expert, in the debate about the new Dutch Intelligence and Security Services Act.

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

I. ORIGINS AND EARLY DEVELOPMENTS

When it comes to interception of electronic communications, Dutch law initially reflected the basic distinction between lawful interception (LI), which takes place domestically, and signals intelligence (SIGINT), which is about collecting foreign communications. SIGINT may also take place domestically when foreign signals are accessible from domestic locations.[1]

In The Netherlands, lawful interception was initially carried out by the domestic security service, the *Binnenlandse Veiligheidsdienst*, or "BVD." The BVD was established in 1949 and was modeled after the British security service MI5, which means that it is strictly separated from law enforcement. Almost right after it was founded, the BVD became a highly regarded partner of the CIA.[2]

For signals intelligence, the Dutch navy, army, and air force each had their own sections, which in 1988 were merged into the new military intelligence service (*Militaire Inlichtingendienst*, or "MID"). These sections only collected SIGINT for military purposes, except for navy intelligence, which operated world-wide and collected political and economic information as well. The MID had its own codebreaking center, which once had been able to break the diplomatic ciphers of Belgium, Germany, Italy, and Turkey and could also read communications from various countries in the Middle East.[3]

All non-military intercepts were provided to the Dutch foreign intelligence service (*Buitenlandse Inlichtingendienst*, or "BID"; since 1971, this organization has been called the *Inlichtingendienst Buitenland*, or "IDB"). This organization, established in 1946, also conducted espionage for the benefit of big Dutch companies, but at the time that was not seen as a problem.[4]

> ***The Dutch Constitution plays almost no role when it comes to electronic surveillance.***

In these early decades, the legal framework for the Dutch secret services was minimal: both the BVD and the BID were created and governed by a classified royal decree. This decree merely instructed the BVD to gather information about people and organizations that could pose a threat to The Netherlands or to friendly foreign powers. The task of the BID was to collect information abroad to support Dutch foreign policy.[5]

The royal decree did not mention any specific powers or methods to be used, so when the BVD wanted to conduct a wiretap, this was justified only by its general mandate.[6] In the 1960s, however, the government became worried about increasingly affordable equipment enabling the user to eavesdrop on other people's conversations and phone calls.

To safeguard a reasonable expectation of privacy, the Dutch penal code was changed in 1971 to prohibit eavesdropping by technical means or through a telephone network.[7] An exception was made for the BVD, but only after prior approval by the Prime Minister and three other ministers. This had already been the practice before this was codified in the penal code, but as a matter of discretion rather than of law.[8]

The law did not cover eavesdropping on wireless telephony, however. At the time, wireless communications could be rather easily intercepted by anyone, so people could not reasonably expect much privacy when communicating this way.[9] This contrasted with cable-bound communications, which were only accessible by the telephone companies and therefore provided more privacy. Based upon this idea, the law did not address the legal basis for interception by the Dutch armed forces of radio and satellite communications.[10]

The first Dutch statute to delineate the roles of the intelligence services was the Intelligence and Security Services Act from 1987 (*Wet op de inlichtingen- en veiligheidsdiensten*, or "Wiv 1987").[11] However, the Act, like the royal decree, merely listed the tasks of the BVD, the IDB, and the military services without specifying, let alone limiting, their powers. The only exception was that they were only allowed to collect, register, and distribute personal data as far as it was necessary to fulfill their lawful tasks.[12]

The Dutch Constitution plays almost no role when it comes to electronic surveillance. In Article 13, it protects the secrecy of correspondence and, since 1983, that of telegraph and telephone communications. However, only the opening of letters and packages must be authorized by a judge; other infringements may be authorized administratively without judicial approval.[13]

Because Dutch courts are allowed to test laws against only treaties and not against the Constitution,[14] the European Convention on Human Rights (ECHR) became the most important driver for developments in The Netherlands.

In this case, the key provision is Article 8, which says that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[15] However, Article 8 continues to explain that the government can limit this right if the limitation is "in accordance with the law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[16] Exactly when these limitations apply is decided by the case law of the European Court of Human Rights (ECtHR).

Thus, in 1994, the Dutch Council of State ruled that the Wiv 1987 was not compliant with Article 8 of the ECHR because it didn't specify in which cases and under which circumstances each investigative method could be used.[17] That prompted the Cabinet to prepare a completely new law. The timing was fortuitous: the government had also decided that the BVD (the domestic security service) should take over the foreign intelligence mission of the IDB (the civilian foreign intelligence service), which had been dissolved a few years earlier because of its failure to coordinate with its customers at other government departments. It was also affected by longstanding conflicts among its staff, which the Prime Minister's department was unable to resolve.[18]

II. THE GENERAL REORGANIZATION OF 2002

After almost three years of deliberation in Parliament, the new Intelligence and Security Services Act (Wiv 2002) came into effect on May 29, 2002. For the first time, the various investigatory powers were specified along with safeguards and general norms for their implementation. Where the Wiv 1987 had just 26 articles, the new law had 106, and most of them have been copied into the current Wiv 2017, so they still apply today.

The law also reorganized the Dutch services: The BVD was turned into the General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst*, or "AIVD") and also became responsible for foreign intelligence on civilian topics. Its primary tasks are investigating individuals and organizations who impose a threat to national security, as well as conducting investigations about other countries on topics determined by the Prime Minister and the Ministers of Foreign Affairs and Defense.[19]

Similarly, the MID was renamed as the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst*, or "MIVD") to better reflect its additional responsibility for military security. Its initial task of providing intelligence about the armed forces of foreign powers was supplemented with investigations to support international crisis management and peace-keeping missions. The MIVD also enacted a separate foreign intelligence mission to address military-related topics.[20]

In general, the Wiv 2002 said that these tasks should be necessary for national security, a criterium which was derived from ECHR Article 8 and which is therefore subject to the case law of the European Court.[21] The Dutch Parliament did not want national security to include "vital economic interests of the Netherlands," which the Cabinet had proposed.[22]

It is important to note that since the enactment of the Wiv 2002, each of the Dutch secret services combine domestic security and foreign intelligence tasks. This is different from many other countries, where these tasks are often conducted by separate agencies and covered by different laws, usually with strict regulations for monitoring their own citizens and less strict or even no rules for foreign intelligence operations.[23] This is because there is just one legal framework in The Netherlands, so both domestic and foreign operations are governed by the same provisions and safeguards.[24] This means there is no need to differentiate between the nationality of targets or to separate foreign and domestic communications, which has turned out to be a problem for the U.S. NSA[25] and for the German foreign intelligence service BND.[26]

It is important to note that since the enactment of the Wiv 2002, each of the Dutch secret services combine domestic security and foreign intelligence tasks. This is different from many other countries.

The Wiv 2002 contained an exclusive list of investigatory powers, which were in fact a codification of what the services were already doing in practice.[27] There are general powers and special powers. General powers range from using open-source information to acquiring information from informants and foreign partners and do not require external approval. The special powers are more intrusive and therefore need prior authorization by the responsible minister.[28] Prior authorization is generally valid for a maximum of three months, after which an extension for the same period can be requested for as long as necessary.

Except in the case of opening letters and packages, there was no authorization required by an independent judge. A request for authorization had to, and still must, satisfy three general norms which the Wiv 2002 introduced for the use of special powers:[29]

1. Necessity: a method must be necessary to fulfill the mission as described by the law, which means there must be a threat to national security that cannot be mitigated otherwise.
2. Proportionality: the consequences of a certain method may not result in a disproportionate disadvantage for the person concerned compared to the goal that is pursued.
3. Subsidiarity: a method may only be used when the goal cannot be achieved in a way that is less intrusive for the person concerned.

Besides powers for human intelligence operations, the Wiv 2002 specified the following special powers for collecting electronic data and communications:

- Accessing computers and computer systems, better known as hacking.[30] This power covers targeted interception, which not only includes telephone and internet taps and the use of directional microphones, but also interception of radio traffic.[31] No external authorization was required for the interception of military radio channels.[32]
- Exploration ("search") of wireless communications to or from other countries.[33] Because content was only collected through short and random snapshots, no external authorization was required.[34]
- Untargeted or bulk interception of wireless telecommunications to or from other countries.[35] Authorization by a minister was not required for storing these data, but only when analysts selected specific content by using selectors like phone numbers, email addresses, and keywords.[36]
- Requesting subscriber information and metadata for individual targets from telecommunications providers, which had to be authorized only internally.[37]

Under the Wiv 2002, the secret services could also request any company or government agency to hand over stored data, but these parties were not obliged to comply. Meanwhile, however, the use of cloud storage became common and so the Wiv 2017 introduced a new article containing an obligation for any party to hand over stored data or communications at the services' request. Given this obligation's high impact on the target's privacy, this requires prior authorization by a minister.[38]

III. NEW & EXISTING OVERSIGHT COMMISSIONS

The Wiv 2002 also introduced a new, independent oversight body called Review Commission for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*, or "CTIVD"). This commission has access to the buildings of the AIVD and MIVD and is allowed to question AIVD and MIVD employees and look into their files, computer systems, and archives, which at the time made the CTIVD one of the best-equipped oversight bodies in the world.[39] The public reports about its in-depth investigations provide a sometimes remarkably detailed insight into the work of the Dutch services.[40] Over the years, there has grown broad appreciation and respect for the expertise and quality of the work of the CTIVD.[41]

Besides the CTIVD, there is also the parliamentary commission for the Intelligence and Security Services (*Commissie voor de Inlichtingen- en Veiligheidsdiensten*, or "CIVD"), which was established in 1952 and was one of the first parliamentary oversight commissions in the world.[42] Beginning in 2003, membership of the commission was open to the parliamentary leaders of all (nine) political parties represented in the lower chamber of parliament. In 2016, however, membership was scaled back to the five largest parties; the exact reason for the change was not disclosed.[43] Because there were concerns about the efficacy of the CIVD, experts proposed to add specialized members of parliament. Instead, the commission decided to add a full-time advisor and improve the flow of information from the agencies.[44]

IV. OPERATIONAL CAPABILITIES

By specifying the various investigatory powers, their safeguards, and the new independent oversight commission, the Wiv 2002 largely met the requirements imposed by the European Court. But it basically allowed the services to continue what they had already been doing, rather than adjust the rules to account for the rapid emergence of the internet the increasing predominance of submarine fiber-optic cables over satellite links for intercontinental communications.

This technological shift coincided with the start of the Global War on Terror after the attacks of September 11, 2001. The Dutch government responded to the attacks with an action plan that included increasing the satellite interception capability.[45] Satellites were still important for military and diplomatic communications, especially in remote areas, where terrorist organizations like Al-Qaeda used them as well. To realize this plan, it was decided to create a new national signals intelligence organization (*Nationale Sigint Organisatie*, or "NSO"), the formation of which started in 2003 and was finished in 2007.[46] The NSO was part of the MIVD, but it also worked for the AIVD and was therefore less independent than the U.S. NSA.

V. SIGINT OPERATIONS BY THE NSO

The NSO began with replacing the satellite intercept station at Zoutkamp, which had just two dishes, with a new facility near the village of Burum, which became fully operational in 2008 and has 15 satellite dishes.[47] The NSO also incorporated the mobile SIGINT units, which are deployed at military operations abroad, as well as the high-frequency radio interception station at Eibergen, which was completely modernized around 2010.[48] Press disclosures indicate that the NSO has contributed significantly to anti-piracy and counterterrorism missions, filling collection gaps of the NSA, and other allied services.[49] Another press report suggested that the NSA had intercepted a large number of Dutch phone calls, which was assumed even by Interior Minister Ronald Plasterk. However, during a court case in early 2014, the government admitted that the number was actually about metadata which the NSO had collected during military missions abroad and subsequently shared with the Americans.[50]

Edward Snowden himself apparently also misunderstood the situation in The Netherlands when he said that the Dutch intelligence services are the "surveillance kings of Europe"[51] — this statement actually applies to the Dutch police force, which conducts about 25,000 taps a year, but therefore rarely conducts undercover observation and bugging operations, which are considered more intrusive and controversial.[52] The annual number of targeted interceptions by the Dutch secret services rose from 559 in 2002 to 1,930 in 2022 for the AIVD and from 19 in 2004 to 704 in 2022 for the MIVD.[53]

No other statistics about data collection are published, but the AIVD and MIVD each produce an unclassified annual report which describes threats and focus areas in general terms.[54] Sometimes, lower-level regulations and policy documents are publicly available — for example, the agreement establishing the Joint Sigint Cyber Unit (JSCU) in 2014,[55] and some additional safeguards which were implemented after the government lost the referendum of 2018 (*see* below).[56]

VI. CYBER OPERATIONS BY THE JSCU

In 2014, the JSCU was created to integrate signals intelligence collection by the NSO with the hacking expertise of the AIVD. With these combined capabilities, the JSCU can be seen as the Dutch equivalent of the U.S. NSA and Government Communications Headquarters (GCHQ), albeit much smaller, as it started with some 350 employees. Like the former NSO, it is not an independent organization, but a joint unit of the AIVD and MIVD. Nonetheless, the JSCU is considered among world's top five cyber powers, capable of creating hacking tools just as sophisticated as those of GCHQ, for example.[57]

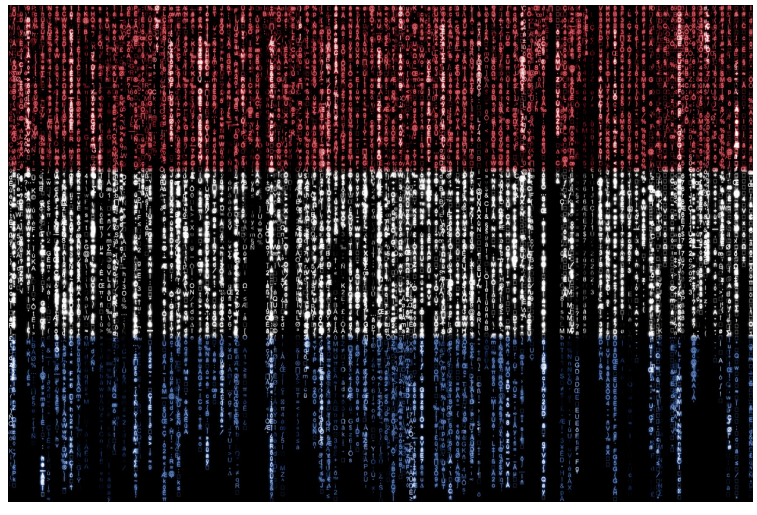
In January 2018, press reports revealed that in 2014 the JSCU successfully infiltrated a Russian hacking group known as Cozy Bear, or APT29. Having access to their computer network, the Dutch observed how the Russians hacked major targets in the United States such as the Democratic National Committee (DNC) and the unclassified networks of the State Department and the White House. The JSCU even managed to hack a security camera in the corridor leading to Cozy Bear's workspace, which allowed it to identify the Russian hackers.[58] Eventually, the AIVD tied Cozy Bear to the Russian foreign intelligence agency SVR and alerted its American counterparts in the summer of 2015.[59]

> ***For a small country like The Netherlands, cooperation and intelligence exchanges with foreign powers is often considered to be of vital importance.***

VII. INTERNATIONAL COOPERATION & OVERSIGHT

For a small country like The Netherlands, cooperation and intelligence exchanges with foreign partners is often considered to be of vital importance. At the BVD, the rule of thumb was that one-third of information comes from open-source, one-third from your own collection efforts, and one-third from partner agencies.[60]

Since such international cooperation is one of the most sensitive and closely guarded secrets, the general public was not aware of it until the Snowden revelations, which illustrated that Dutch military intelligence works closely with the NSA. The AIVD is also not a small player, and over the years it has built up an excellent reputation among its foreign partners.[61]



This international cooperation usually falls outside the mandate of the national intelligence oversight bodies. In 2014, the chairman of the Dutch CTIVD had already taken the initiative for cooperation between the oversight bodies from Belgium, Denmark, Norway, and Switzerland in order to exchange experiences and methods to fill this growing oversight gap.[62] In 2019, the British oversight authority IPCO also joined this group, which then established itself as the Intelligence Oversight Working Group.[63]

VIII. TOWARDS A NEW LAW WITH EXPANDED POWERS

With an exponential growth of internet communications, it was felt that without access to internet backbone cables, the Dutch intelligence and security services would become "deaf and blind."[64] This was also recognized by the independent Dessens Commission, which conducted the first evaluation of the Wiv 2002. This commission began its work in February 2013, but when it published its report on December 2, things had changed dramatically because of the Snowden revelations that had started in June of that year.

The Dessens Commission recommended to provide the Dutch services with the power they were hitherto deprived of by the Wiv 2002: untargeted interception of cable-bound communications. But, according to Snowden, this was exactly one of the methods which the NSA and GCHQ allegedly abused for indiscriminate mass-surveillance.[65]

The bulk collection of cable-bound communications was implemented by making the existing provision that applied to only wireless communications "technology independent."[66] This means that the rules apply regardless of the communications technology being used, which was a general aim for the new law in order to make it future-proof in a world in which technology develops much faster than laws.

The Wiv 2017 also expanded the hacking power by allowing the hacking of computer systems used by third parties whenever necessary to get access to data of the intended target. Although this received less attention than the bulk cable tapping, it gives the JSCU the same controversial power which GCHQ used in 2010 to hack the network of the Belgian telecommunications company Belgacom as a means to gain access to targets elsewhere.[67]

A much less-noticed new feature of the Wiv 2017 is the integrated directive (*Geïntegreerde Aanwijzing*, or "GA"). In this classified document, the Prime Minister, Interior Minister, Defense Minister, Foreign Minister, and Justice Minister describe the intelligence needs, their priority, and their degree of coverage for the next four years. Under the Wiv 2002, there was only such a directive for the foreign intelligence missions of both services while the AIVD determined the priorities for threats to domestic security on its own, based upon its tasks provided by the law. The Wiv 2017 removed this difference between foreign and domestic topics and now the GA encompasses all tasks.[68]

The Wiv 2017 also expanded the hacking power by allowing the hacking of computer systems used by third parties whenever necessary to egt access to data of the intended target.

IX. NEW SAFEGUARDS

To address the concerns in society, the Cabinet had introduced a new kind of safeguard in the form of an independent review commission (Toetsingscommissie Inzet Bevoegdheden, or "TIB"), which must approve all requests for deployment of the most intrusive powers after they have been authorized by one of the ministers. With its ex ante review, this commission is different from the CTIVD, which is responsible for oversight during and after the operations of the Dutch services.

The TIB consists of two former judges and one member with relevant technical expertise, but it was not established as a judicial body because judges may not have jurisdiction over foreign nationals.[69] However, for intercepting communications between lawyers and their clients and between journalists and their sources, there must be prior approval by the district court of The Hague.[70]

A rather complicated set of safeguards was created for the extended power of bulk collection. Now there are three stages, during each of which the AIVD and MIVD need prior authorization from their respective minister, followed by approval by the TIB. Simplified, these three stages are:

1. Acquisition: data channels of interest are copied from fiber-optic cables and satellite links and their traffic can be stored for up to 3 years.
2. Preparation: this includes finding out the type of traffic as well as finding new selectors related to already known ones.
3. Processing: conducting (automated) analysis of bulk metadata and selecting the content of communications using phone numbers, internet identifiers, and keywords.

X. THE REFERENDUM & THE LATEST DEVELOPMENTS

After the new Intelligence and Security Services Act (Wiv 2017) had been enacted on August 17, 2017, a group of five critical students managed to get enough support for an advisory referendum about the new law — the first and so far only referendum in the world on intelligence and security services. Arguments made against the law included the threat to privacy by broader hacking powers and the exchange of data with foreign partners. Most critized was the untargeted cable tapping, which adversaries successfully framed as a "dragnet" able to pull in communications of millions of innocent citizens and thereby creating a chilling effect on free speech.[71] Digital rights activists, scholars, and supporters of the law held many debates and lectures around the country,[72] and on March 21, 2018, it turned out that 49.4 percent of the votes were against and 46.5 percent were in favor of the new law, with 4 percent blank votes.[73]

In response, the lower chamber of Parliament insisted on an additional legal safeguard: the implementation of both the general and the special powers now must be "as targeted as possible," which is interpretated to mean that "information that is not strictly necessary for an investigation has to be reduced to a minimum, given the technical and operational circumstances of the case."[74]

Soon, reports by the oversight commission CTIVD made clear that the Wiv 2017 was not as future-proof as intended. Not only can untargeted cable tapping result in the collection of huge amounts of data, but this also happens through so-called bulk hacks in which the JSCU acquires very large sets of data which are then kept indefinitely.[75]

Very large sets of data, such as data containing airline passenger information, are also acquired through informants,[76] while large quantities of open-source information are queried by using automated tools.[77] Because these are general powers, all of this happens without authorization by the requisite minister and subsequent approval by the TIB.

These issues were also identified in the extensive report of an independent commission that in 2020 evaluated the implementation of the Wiv 2017 and recommends, among many other things, new and uniform provisions for bulk data sets regardless of how they are acquired. This could include prior approval for their acquisition and applying stricter rules for data from untargeted interception and bulk data sets from other sources, which would mean limiting analysts' access, limiting the retention period, and applying safeguards for sharing with foreign partners.[78] The commission also recommended a separate provision for exploring telecommunication networks before the actual interception process.[79] Besides technical complications, the lack of such a provision appeared to be one of the reasons that bulk cable tapping did not become operational until four years after the Wiv 2017 came into force.[80]

X. CONCLUSION

The Netherlands is a small country, but its intelligence and security services are valued by its foreign partners for being "technically competent and highly motivated."[81] Since 2002, its operations have been regulated by a detailed law in order to meet the requirements of the European Human Rights Convention. But when targets had to be found among a rapidly increasing volume of internet traffic, the fact that the Wiv 2002 offered no opportunity for bulk collection of cable-bound communications was viewed as a significant limitation.

This was repaired by the current law, but it came with a complex system of safeguards that did not align with current practices. Because of this focus on untargeted interception, the increasing impact of hacking operations and bulk data sets had been ignored.[82] This means that already within five years after its enactment, a substantial reform of the Wiv 2017 is necessary, and during such reform the most important investigatory powers and their safeguards must be balanced once again.

What might this entail? For bulk data sets, the law should apply a uniform regime, regardless of their origin, while for hacking operations the Dutch services probably need more leeway to keep up with the speed of their adversaries.[83] Safeguarding privacy rights may then require a new form of real-time oversight, which means the relationship between the old and the new oversight body would need adjustment as well. Finally, untargeted cable tapping needs further evaluation, as this method only recently became operational.

ENDNOTES

1. Timothy H. Edgar, *Beyond Snowden, Privacy, Mass Surveillance and the Struggle to Reform the NSA*, Brookings Institution Press, Washington, D.C., 35 (2017).
2. *See, e.g.*, Cees Wiebes, *Samen met de CIA. Operaties achter het IJzeren Gordijn*, Uitgeverij Boom, Amsterdam 2016.
3. Cees Wiebes, *Dutch Sigint during the Cold War, 1945-94*, in: Matthew M. Aid & Cees Wiebes, *Secrets of Signals Intelligence during the Cold War and Beyond*, London, 276–78 (2001).
4. Bob de Graaff & Cees Wiebes, *Villa Maarheeze, de geschiedenis van de inlichtingendienst buitenland*, Sdu Uitgevers, Den Haag, 295 (1998).
5. Koninklijk Besluit (KB) nr. 51 from August 8, 1949, which was eventually published in 1972, available at https://www.inlichtingendiensten.nl/organisatie/kb1949.pdf.
6. A. H. Ekker, *Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten*, Computerrecht 77–83 (2002), https://pure.uva.nl/ws/files/3536289/24664_onderscheppen_van_telecommunicatie.html; *see also* MvT Wiv 2002, at 40.
7. Articles 139a to 139c Wetboek van Strafecht, in force as of April 23, 1971. See Kamerstukken 1967/1968, dossiernr. 9419, nr. 3, Memorie van Toelichting, https://repository.overheid.nl/frbr/sgd/19671968/0000240283/1/pdf/SGD_19671968_0002731.pdf.
8. *See* Handelingen van de Tweede Kamer der Staten Generaal, zitting 1963-1964, pp. 435–36, https://repository.overheid.nl/frbr/sgd/19631964/0000252688/1/pdf/SGD_19631964_0000379.pdf.
9. *See* Kamerstukken 1966/1967, dossiernr. 8911, nr. 3, Memorie van Toelichting, p. 6, https://repository.overheid.nl/frbr/sgd/19661967/0000244271/1/pdf/SGD_19661967_0001328.pdf.
10. Ekker 2002. The explanation by Professor Bart-Jaap Koops during an expert meeting organized by the Dutch Senate on June 5, 2014 can be found at https://www.eerstekamer.nl/behandeling/20140605/verslag_van_een_expertmeeting.
11. Law of December 3, 1987, Stb. 635; entry into force on February 1, 1988, https://www.inlichtingendiensten.nl/organisatie/wiv1987.pdf.
12. According to Article 16 of the Wiv 1987.
13. E. J. Koops & R. Passchier, *Wetenschappelijk commentaar op de grondwet - Artikel 13 - Vertrouwelijke communicatie*, Nederland Rechtsstaat (March 2020), https://scholarlypublications.universiteitleiden.nl/access/item%3A2966647/view
14. According to Articles 94 and 120 of the Constitution.
15. European Convention on Human Rights, as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, art. 8 (1950), https://www.echr.coe.int/documents/convention_eng.pdf.
16. *Id*.
17. Raad van State, *Afdeling Bestuursrechtspraak*, June 16, 1994 (AB 1995, 238); Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen*, Den Haag, 24–26 (Dec. 2, 2013), https://www.aivd.nl/documenten/rapporten/2013/12/02/rapport-commissie-dessens-met-evaluatie-wiv-2002.
18. De Graaff & Wiebes, supra note 4, at 402–09, 411–21.
19. Wiv 2002, art. 6; Wiv 2017, art. 8. The AIVD is headquartered in Zoetermeer and currently has some 2,000 employees.
20. Wiv 2002, art. 7; Wiv 2017, art. 10. The MIVD is headquartered in The Hague and currently has some 1,000 employees.
21. Ekker 2002; Commissie Dessens, 29–30.
22. Commisie Dessens, 30.
23. For more about this distinction, *see* Sergei Boeke, Reframing 'mass surveillance', in Terrorists' Use of the Internet, IOS Press, 307–18 (2017).
24. When collection takes places during military missions abroad, the Dutch law is applied analogously. *See* Commissie Dessens, 98.
25. *See, e.g.*, Barton Gellman, Julie Tate, & Ashkan Soltani, *In NSA-intercepted data, those not targeted far outnumber the foreigners who are*, The Washington Post (July 5, 2014), http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.
26. Peter Koop, *New details about the selectors NSA provided to BND*, Electrospaces.net (Nov. 3, 2015), https://www.electrospaces.net/2015/11/new-details-about-selectors-nsa.html.
27. Rob Dielemans, *De Wiv 2002 en Wiv 2017 p enkele hoofdlijnen vergeleken*, in Justitiële verkenningen, Jrg. 44, nr. 1: *Geheime diensten en de democratische rechtsstaat*, Boom juridisch, Den Haag, 70 (2018).
28. Nico van Eijk & Quirine Eijkman, *Enkele kanttekeningen bij de Wiv 2017*, in Justitiële verkenningen, Jrg. 44, nr. 1: *Geheime diensten en de democratische rechtsstaat*, Boom juridisch, Den Haag, 103–04 (2018).
29. Wiv 2002, arts. 18, 32; Commissie Dessens, 36.
30. Wiv 2002, art. 24; Wiv 2017, art. 45.
31. Wiv 2002, art. 25; Wiv 2017, art. 47.

32. CTIVD, *Toezichtsrapport inzake de inzet van SIGINT door de MIVD*, nr. 28, 12–13 (Aug. 23, 2011).
33. Wiv 2002, art. 26; Wiv 2017, art. 49.
34. CTIVD, *supra* note 33, at 21.
35. Wiv 2002, art. 27; Wiv 2017, arts. 48–50.
36. CTIVD, *supra* note 33, at 16.
37. Wiv 2002, arts. 28, 29; Wiv 2017, arts. 55, 56.
38. Wiv 2017, art. 54. This power is quite similar to that of the NSA under the PRISM program, except that the Dutch services can use it for domestic targets as well.
39. R. H. T. Jansen, *Toezicht onder de Wet op de inlichtingen- en veiligheidsdiensten 2017. Een tour de force*, in Nederlands Tijdschrift voor de Mensenrechten. NJCM-Bulletin, 46, 4, (2021), https://repository.ubn.ru.nl/handle/2066/237916?_ga=2.191487151.429724145.1641718720-2074815222.1641718720.
40. The CTIVD investigation oversight protocol can be found at https://english.ctivd.nl/oversight/documents/publications/2019/06/19/oversight-protocol.
41. Commissie Dessens, 59.
42. In Germany such a commission followed in 1956, in the US in 1975, and in France and the UK only in the 1990s. *See* Constant Hijzen, *Vijandbeelden, De veiligheidsdiensten en de democratie*, 1912-1992, Uitgeverij Boom, Amsterdam, 126–28 (2016).
43. R. H. T Jansen, *Parlementaire controle op de inlichtingen- en veiligheidsdiensten in Nederland*, in Rechtsgeleerd Magazijn THEMIS, 184–85 (2019), https://repository.ubn.ru.nl/bitstream/handle/2066/214693/214693pub.pdf.
44. *Id.* at 189–90.
45. *Brief aan de Tweede Kamer der Staten-Generaal naar aanleiding van de Terroristische aanslagen in de Verenigde Staten*, TK 27.925, nr. 10, 11 (Oct. 5, 2001), https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vi3ajy7vxxz0.
46. *NSO wil de diensten van dienst zijn*, in INGELICHT, Informatiemagazine voor de Militaire Inlichtingen en Veiligheidsdienst, nr. 4, 10–11 (Aug. 2007).
47. Jan Abrahamse, *It Greate Ear in Burum*, Noorderbreedte.nl (Nov. 30, 2006), https://www.noorderbreedte.nl/2006/11/30/it-greate-ear-in-burum/.
48. Details about the Eibergen station can be found at https://www.cryptomuseum.com/intel/svic/#eibergen.
49. *The secret role of the Dutch in the American war on terror*, NRC (March 5, 2014), https://www.nrc.nl/nieuws/2014/03/05/the-secret-role-of-the-dutch-in-the-american-war-on-terror-a1426677.
50. Peter Koop, *Dutch government tried to hide the truth about metadata collection*, Electrospaces.net (Feb. 17, 2014), https://www.electrospaces.net/2014/02/dutch-government-tried-to-hide-truth.html.
51. Snowden: *AIVD en MIVD zijn ondergeschikt aan de VS*, Nieuwsuur (Jan. 21, 2015), https://nos.nl/nieuwsuur/artikel/2014570-snowden-aivd-en-mivd-zijn-ondergeschikt-aan-de-vs (as of 11:30 in the embedded video).
52. *See* G. Ordinot et al., *Het gebruik van de telefoon- en internettap in de opsporing*, WODC, Boom Lemma uitgevers, Meppel, 104, 173–74 (2012), https://repository.wodc.nl/bitstream/handle/20.500.12832/1254/ob304-volledige-tekst_tcm28-71492.pdf.
53. For the AIVD, *see* https://www.aivd.nl/onderwerpen/afluisteren/tapstatistieken; for the MIVD, *see* https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/tapstatistieken.
54. The annual reports also contain numbers about notifications to former subjects of investigation, background investigations, and complaints against the services.
55. *Kamerbrief en convenant JSCU*, July 3, 2014, https://www.aivd.nl/documenten/kamerstukken/2014/07/03/kamerbrief-en-convenant-jscu.
56. *Beleidsregels Wiv 2017*, April 25, 2018, https://wetten.overheid.nl/BWBR0040860/2018-05-01.
57. Huib Modderkolk, *Het is oorlog maar niemand die het ziet*, Podium Uitgeverij, Amsterdam, 242 (2019).
58. Huib Modderkolk, *Dutch agencies provide crucial intel about Russia's interference in US-elections*, De Volkskrant (Jan. 25, 2018), https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/.
59. Modderkolk, *supra* note 58, at 176–92.
60. According to Arthur Docters van Leeuwen, head the BVD from 1989 to 1995. Arthur Docters van Leeuwen & Lars Kuipers, *Een spoor van vernieuwing*, Uitgeverij Prometheus, Amsterdam, 188 (2020).
61. According to Dick Schoof, head of the AIVD from 2018 to 2020. Paul H. A. M. Abels, *Spionkoppen, Inlichtingenleiderschap in elf portretten*, Uitgeverij Prometheus, Amsterdam, 301 (2020).
62. Wouter de Ridder, *A simple yet existential demand: let oversight bodies work together*, November 6, 2019: https://aboutintel.eu/simple-oversight-demands/.
63. *Charter of the Intelligence Oversight Working Group*, December 12, 2019, https://english.ctivd.nl/documents/publications/2019/12/12/index.
64. Commissie Dessens, *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen*, 77 (Dec. 2, 2013).
65. *See, e.g.*, Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies & James Ball, *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian (June 21, 2013), https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. These reports usually failed to put these collection methods in the context of the full intelligence cycle from priorization to analyzation.

66. Commissie Dessens, 76.
67. Known as Operation Socialist. See, e.g., Ryan Galagher, The Inside Story of How British Spies Hacked Belgium's Largest Telco, The Intercept (Dec. 13, 2014), https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.
68. This sparked some concern that the AIVD could be directed to provide politically desirable intelligence instead of "speaking truth to power." See P. H. A. M. Abels, *Per Undas Adversas? Geheime diensten in de maalstroom van politiek en beleid*, oratie Universiteit Leiden (Feb. 16, 2018).
69. Dielemans, *supra* note 28, at 78.
70. As required by Dutch courts and the ECtHR, November 27, 2012 (Telegraaf Media Groep v. The Netherlands).
71. A list of the reactions by various organizations on the new law can be found here: https://blog.cyberwar.nl/2015/09/dutch-lijstje-van-reacties-van-organisaties-op-de-wiv-consultatie/.
72. *See, e.g.*, Paul Abels, *Een referendum dat er toe doet: terugblik op drie weken WIV-debatten*, Referendum Wet op de inlichtingen- en veiligheidsdiensten Weblog (March 22, 2018), https://wivreferendum.weblog.leidenuniv.nl/2018/03/22/een-referendum-dat-er-toe-doet-terugblik-op-drie-weken-wiv-debatten/.
73. Kiesraad, *Uitslag referendum over Wiv: meerderheid tegen*, March 29, 2018, https://www.kiesraad.nl/actueel/nieuws/2018/03/29/uitslag-referendum-over-wiv-meerderheid-tegen.
74. CTIVD, *Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD - De snapshotfase*, nr. 75, 37–38 (Jan. 26, 2022), https://www.ctivd.nl/documenten/rapporten/2022/03/15/index.
75. CTIVD, *Toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*, nr. 70 (Sept. 22, 2020), https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-bulkhacks/documenten/rapporten/2020/09/22/rapport-70.
76. CTIVD, *Toezichtsrapport over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD*, nr. 71 (Sept. 22, 2020), https://www.ctivd.nl/onderzoeken/aivd-mivd-onderzoek-passagiersgegevens/documenten/rapporten/2020/09/22/rapport-71.
77. CTIVD, *Toezichtsrapport over automated OSINT door de AIVD en de MIVD*, nr. 74 (Feb. 8, 2022), https://www.ctivd.nl/documenten/rapporten/2022/02/08/rapport-74.
78. Commissie Bos-Jones, *Rapport van de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017*, 153 (Jan. 20, 2021), https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z01039&did=2021D02502.
79. *Id.* at 155.
80. See CTIVD, *Brief CTIVD over verscherpt toezicht op de kabel*, 2 (June 27, 2022), https://www.ctivd.nl/actueel/nieuws/2022/06/27/index; CTIVD, supra note 76.
81. According to an internal document from GCHQ cited in Julian Borger, *GCHQ and European spy agencies worked together on mass surveillance*, The Guardian (Nov. 1, 2013), https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.
82. The British Investigatory Powers Act (IPA) of 2016, often mocked as "the snoopers charter," covers all these topics in equal detail. *See* Home Office, *Investigatory Powers Act 2016* – codes of practice, Gov.UK (12 June 2018, updated 19 April 2023), https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.
83. *See* the proposal from April 1, 2022 for a temporary new law to counter offensive foreign cyber operations, which can be accessed at *Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma*, https://wetgevingskalender.overheid.nl/Regeling/WGK013565#.