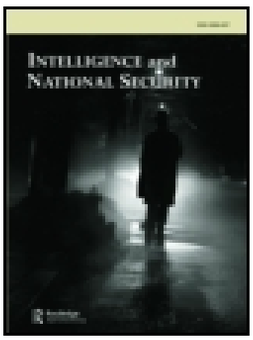

Intelligence and National Security

ISSN: 0268-4527 (Print) 1743-9019 (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

Maximator: European signals intelligence cooperation, from a Dutch perspective

Bart Jacobs

To cite this article: Bart Jacobs (2020): Maximator: European signals intelligence cooperation, from a Dutch perspective, Intelligence and National Security, DOI: 10.1080/02684527.2020.1743538

To link to this article: https://doi.org/10.1080/02684527.2020.1743538

Published online: 07 Apr 2020.

INTELLIGENCE AND NATIONAL SECURITY
https://doi.org/10.1080/02684527.2020.1743538

Routledge
Taylor & Francis Group

ARTICLE

Maximator: European signals intelligence cooperation, from a Dutch perspective

Bart Jacobs

ABSTRACT

This article is first to report on the secret European five-partner sigint alliance Maximator that started in the late 1970s. It discloses the name Maximator and provides documentary evidence. The five members of this European alliance are Denmark Sweden, Germany, the Netherlands, and France. The cooperation involves both signals analysis and crypto analysis. The Maximator alliance has remained secret for almost fifty years, in contrast to its Anglo-Saxon Five-Eyes counterpart. The existence of this European sigint alliance gives a novel perspective on western sigint collaborations in the late twentieth century. The article explains and illustrates, with relatively much attention for the cryptographic details, how the five Maximator participants strengthened their effectiveness via the information about rigged cryptographic devices that its German partner provided, via the joint U.S.-German ownership and control of the Swiss producer Crypto AG of cryptographic devices.

1. Introduction

The post-Second World War signals intelligence (SIGINT) cooperation between five Anglo-Saxon countries – Australia, Canada, the United Kingdom, New Zealand, and the United States – is well-documented.[1] This alliance is often called *Five Eyes* and is based on the 1946 UKUSA Agreement. What is not publicly known so far is that there is a second, parallel, western signals intelligence alliance, namely in north-western Europe, also with five members. It has existed since 1976 and is called Maximator. It comprises Denmark, France, Germany, Sweden, and the Netherlands and is still active today. The Maximator alliance deepens our understanding of the recently-revealed operation Thesaurus/Rubicon: the joint CIA-BND ownership and control of the Swiss manufacturer of cryptographic equipment Crypto AG, from 1970 to 1993.[2] Crucial information about the inner workings (and weaknesses) of cryptographic devices sold by Crypto AG (and by other companies) were distributed within the Maximator network. This allowed the participants to decrypt intercepted messages from the more than one hundred countries that had bought compromised devices from the 1970s onwards.

The first and main part of this article provides historical evidence about this Maximator alliance and provides some background information, obtained from sources in the Dutch intelligence community. This picture is far from complete and in need of extension via future research, especially based on information from other participating countries. The information about the existence and composition of the Maximator alliance is based on three independent sources from the Dutch intelligence community and is supported by several documents – see Figures 1 and 2 below. The more detailed information about Maximator and its Dutch arm, TIVC, in Section 3 is based on individual sources.[3]

CONTACT Bart Jacobs bart@cs.ru.nl

Figure 1. Cover pages of booklets of several Maximator meetings. The page of the meeting at Rheinhausen – home to a BND satellite listening post (Schmidt-Eenboom, 'The Bundesnachrichtendienst, the Bundeswehr and SIGINT'.) – is most informative, since it includes the flags of the five countries forming the Maximator alliance. Edison is the codename for the Netherlands; this meeting took place in Amsterdam: the bottle in the picture carries three crosses (x) on top of each other, which forms the logo of the city of Amsterdam.

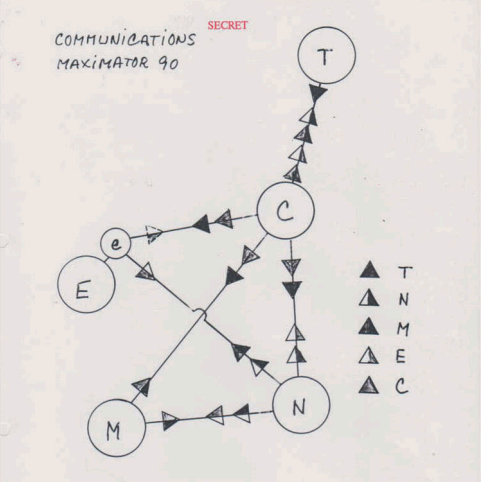

Figure 2. Sketch of the communication lines between the Maximator partners in 1990, using letters for the code names of the participating countries: T = Thymian = Sweden, C = Concilium = Denmark, E = Edison = The Netherlands, M = Marathon = France, N = Novalis = Germany. The small letter 'e' on the Dutch side refers to Erasmus, which was the code name for the 898th Army signals battalion, stationed at Eibergen, home to a HF listening post. The triangles seem to indicate how information (esp. intercepts) can flow from one party to another. At the time the diagram was drawn (1990) there was no direct E-M connection, but it did exist later.

2. Maximator

The Maximator alliance began in 1976 at the initiative of Denmark. It initially involved, besides Denmark, only Sweden and Germany. The Netherlands was invited to join in 1977 and did so in 1978. Bilateral cooperation in signals intelligence already existed between most (pairs) of these initial four countries. One motivation to start cooperating more broadly was the emergence of signals intelligence via satellites, which required substantial investment. A second motivation was to jointly work on technical interception challenges and exchange methods. The idea was to combine forces and divide tasks in order to reduce costs and so become more effective. The cooperation involved both cryptanalysis and signals analysis – from the ether only, via SHF (satellite) and HF (short-wave) traffic. France's request to join in 1983 was supported especially by Germany, since the (signals) intelligence

cooperation between France and Germany was strong, having started soon after the Second World War based on close contacts between leading figures Gustave Bertrand and Reinhard Gehlen.[4] As a result, France was invited in 1984 and joined in 1985.

The name Maximator refers to a beer brand from the southern German region of Bavaria (see image 1, below). Bavaria's capital is Munich, and its suburb Pullach was, until 2017, home to the *Bundesnachrichtendienst* (BND), the German foreign intelligence agency. At some stage in 1979, representatives of the alliance-in-the-making were having a beer there, while pondering a good name for their emerging cooperation. They looked at their glasses, filled with *Doppelbock* beer of the local brand Maximator[5] and reached a decision.[6]

Once the Maximator alliance had been established with five participating countries – Denmark, France, Germany, Sweden, and the Netherlands – it remained stable and continues to operate today. Other countries have asked whether they could join at some stage, but such requests have been turned down. The cooperation was bottom-up and based on close personal ties and a shared high level of technical and cryptanalytical skills. Certain countries were deliberately not allowed to join because within the Maximator alliance they were considered as lacking relevant (signal-/crypto-analytical) expertise and/or experience. Allegedly, these countries include Norway,[7] Spain and Italy. Other (political) factors may also have played a role in their exclusion. Belgium is a notable exception in north-western Europe; it had not been invited to join Maximator because of its lack of SIGINT (and COMSEC) capabilities.[8]

Within the participating countries specific intelligence organisations played relevant roles. In Germany the *Bundesnachrichtendienst* BND is responsible for (foreign) signals intelligence, whereas what was then called the *Zentralstelle für das Chiffrierwesen* ZfCh did the cryptanalytical work.[9] In Denmark, Sweden, and the Netherlands these activities were combined in respectively the *Forsvarets Efterretningstjeneste* (Danish Defence Intelligence Service DDIS), the *Försvarets radioanstalt* (FRA, National Defence Radio Establishment), and the *Technisch Informatie Verwerkingscentrum* (TIVC, Technical Information Processing Centre).[10] French Maximator activities were part of the *Direction Générale de la Sécurité Extérieure* (DGSE, General Directorate for External Security).[11]

The Maximator cooperation involved both signals analysis and cryptanalysis. The signals analysis part focused on coordinating interception mechanisms and efforts and on exchanging intercepted (encrypted) messages. Signals analysis was discussed in multilateral meetings, involving the entire Maximator alliance (see Figure 1). Cryptanalysis, on the other hand, was discussed only bilaterally.[12] Each participating country was supposed to perform its own decryptions. This is common practice in the intelligence community in order to prevent being fed cooked-up information. The communication channels between the partners in 1990 are described in Figure 2. Dedicated crypto systems were

Image 1. Maximator Beer. Mercator beer brand (attribution: Augustiner Brewery)

used for each of the bilateral connections. The cryptanalytical part of the cooperation involved exchanges of algorithms used in various (deliberately weakened) cryptographic devices used by target countries. It was then left up to the Maximator participants themselves to find out how to exploit weaknesses in the algorithms of these devices. Such exploitations are also called 'solutions'. A common approach was to use so-called correlation attacks on shift registers. This technique became public in the late 1980s[13] but was at that time already quite common in the intelligence community[14] – now chagrined by the publication. In principle, (implementations of) solution methods were not exchanged within Maximator. Occasionally, (long term) cryptographic keys were shared, as outcomes of such solutions.

The focus within Maximator was on interception (and decryption) of diplomatic traffic going through the ether (HF and SHF). In the early days of Maximator, encrypted connections were almost exclusively used for diplomatic and military communication. In the 1980s and 1990s commercial companies slowly started using encryption on their main communication lines. It was only from the late 1990s onwards that encryption became a commodity, for ordinary users, in order to protect their online communications and transactions. This completely changed the landscape.

In the early days of Maximator, encryption was still hardware-based. The transition from rotors to shift registers had mostly happened.[15] Cryptographic algorithms were 'baked into' dedicated chips, and were not yet software-based. There were only a few companies that offered (hardware) encryption devices on the world market. Those companies were mostly controlled by western intelligence organisations, so that many countries outside a small circle received deliberately weakened versions, whose cipher texts could be decrypted by *cognoscienti* with relative ease. The Swiss company Crypto AG is the main example; it supplied its cryptographic devices to around 70-80% of the (non-communist) market, while being secretly owned by the CIA and the BND, as was disclosed in early 2020 by the German ZDF television programme *Frontal 21*[16] and the *Washington Post*, based on leaked CIA and BND documents.[17]

With the right context in mind, one can already recognise the Maximator alliance in these BND documents. The alliance is never mentioned there, especially not by name, but one byline says: *Diese Fähigkeiten blieben nicht auf USA und Deutschland beschränkt; im Laufe der Jahre wurden Staaten wie Dänemark, Frankreich, Großbritannien, Israel, Niederlande, Schweden u.a. in den Kreis der 'cognoscenti' aufgenommen*.[18] For those who already knew about a five-country alliance in continental Europe it is clear from this quote which those five countries are.

As an aside, Aldrich has already mentioned continental European SIGINT cooperation and that '… the Europeans had recently set up their own mini-UKUSA alliance called "The Ring of Five", consisting of the SIGINT agencies of Germany, the Netherlands, France, Belgium and Denmark … '[19] However, this Ring of Five is *not* the Maximator alliance: as mentioned, Belgium is not in Maximator but Sweden is (see the Rheinhausen page in Figure 1). Besides Maximator, whose focus is on diplomatic communications, there seems to be (or, has been) a parallel alliance for intercepting (metadata of) military communications.[20] It contains the five countries listed By Aldrich in his book *GCHQ*. The two alliances – Maximator and the one mentioned by Aldrich – are different but are easily confused.[21]

3. TIVC, the Dutch leg of Maximator

Wiebes provides a short, first history of the Dutch SIGINT organisation TIVC.[22] Here we extend this account with three new perspectives, namely (1) that TIVC formed the Dutch part of the Maximator alliance, (2) that TIVC obtained via Maximator partner the BND information about the algorithms in Crypto AG devices – to which the BND had access via its hidden ownership of the company, and (3) that cryptographic equipment of the Dutch manufacturer Philips was also weakened, with Dutch (partly TIVC) involvement.

As mentioned by Wiebes, TIVC was embedded within the Royal Dutch Navy and operated from the navy barracks at Kattenburg in the centre of Amsterdam. It had separate departments for signals analysis and for cryptanalysis (including linguists). After 2010 these departments became part of the

Joint SIGINT Cyber Unit (JSCU) which is jointly operated by the two intelligence and security services (AIVD and MIVD) in the Netherlands. Signals interception for TIVC came mainly from the HF-antennas at Eemnes and satellite (SHF) dishes at Burum and Zoutkamp in the north of the Netherlands. From 1963 the Netherlands also had an interception station in the Caribbean, at Curaçao, with Venezuela[23] and Cuba as main targets.

As described above, TIVC was an early partner in Maximator. It was a relatively small, but effective SIGINT organisation that claims to have deciphered (mostly diplomatic) communications from almost 75 countries.

3.1. The Falklands war

The Maximator alliance and its member TIVC played a special role in the Falklands war (1982). At the time, the Argentinian navy and diplomatic service used Crypto AG equipment to secure their communications. In particular, they used the devices HC550 and HC570, which belong to the same family and use the same cryptographic algorithm.[24] This algorithm was rigged, jointly by the BND and the CIA, via their ownership of Crypto AG. The details of this algorithm were shared by the BND within Maximator with TIVC. This enabled the Dutch to read Argentinian naval and diplomatic communications before the war started. As reported by Aldrich and Wiebes, the British SIGINT organisation GCHQ had neglected Argentina.[25] It was not able to read communications secured by Crypto AG devices. When the war started, it asked, under pressure, countries on the European continent for help. A directly involved Dutch source states that at that stage a specialist from TIVC travelled to GCHQ and explained how the HC500 Crypto AG devices for Argentinian naval and diplomatic communications worked; subsequent solution of the ciphers was left to GCHQ itself.[26] Looking back, the CIA history says that in 1982 the ability to read Argentine communications became critical to Great Britain's successful prosecution of the Falklands war.[27] A stronger statement occurs in the BND history: '*Da die Briten als ständige Trittbrettfahrer dieser Operation angesehen werden mussten (…) darf behauptet werden, dass der Ausgang des Falkland-Krieges 1982 ganz wesentlich von der hier beschriebenen Operation beeinflusst, wenn nicht sogar entschieden wurde*' – that the outcome of the war was influenced in an essential way, if not decided, by the Rubicon operation.

The fact that GCHQ knew how to break the Argentinian codes is well-known. As Aldrich writes: 'How was GCHQ reading the Argentinean communications with such ease? The answer was quite simple. Some of Argentina's high-grade military and diplomatic communications systems made use of expensive but thoroughly compromised European cypher machines … '[28] A small piece of the puzzle that is added here is the nature of these cypher machines and the route through which GCHQ actually learned about how to break them, namely via the BND, Maximator and TIVC.

At some stage during the war the Argentinians found out that their coded messages were being read. They could not quickly change all equipment, so they decided to change their cryptographic key management – which makes sense. They started refreshing their keys every hour, instead of every three days. This made code breaking much more difficult, since a short period of one hour may not contain enough cipher text to carry out a successful cryptanalytical attack.

There are different stories about how the Argentinians learned about the compromise of their encipherments. The most common explanation is that they found out via member of Parliament Ted Rowlands who revealed in the House of Commons on 3 April 1982, that GCHQ was reading Argentine diplomatic communications. However, another account that circulates in Dutch intelligence circles is that a British pilot shot down by the Argentinians carried information that could only have been obtained via compromised communications.

3.2. Aroflex, Philips and Turkey

Aroflex is the name for a successful electronic encryption device developed by Philips in the Netherlands in the late 1970s. It was approved for use within NATO, by the relevant evaluation

agency SECAN. NATO allowed several countries to use the Aroflex also for their internal communications, but it did not allow commercial sale of the device. For further usage, two modified – rigged, if you like – versions of the Aroflex were developed.

First, a commercial version of the Aroflex device, with an adapted crypto algorithm, was developed under the official name T1000CA, but with the unofficial name Beroflex. TIVC collaborated with Philips in the design of the crypto algorithm for this Beroflex. Both sides came up with their own proposal for modification of the Aroflex. After delibration, TIVC's proposal was selected because it involved the least modification of the existing Aroflex. Still, breaking encipherments involved solving many systems of binary linear equations. This was beyond what general purpose computers could do at the time. TIVC turned to Philips' research department (known as Natlab) which designed a dedicated chip that could solve the equations in about 40 minutes.[29] This chip was built into a special purpose decryption device that was sold to the U.S. and to Maximator partners. The CIA history contains a single line about Beroflex and about this special device to break it: ' … the cryptologic could not be exploited without a Dutch special purpose device which both NSA and the ZfCh were forced to procure'.[30] Thus, the Dutch were not only active (too) in deliberately weakening crypto equipment, in good public-private partnership, but even in developing and selling dedicated devices to break it. This story has recently appeared, via independent sources, in the Dutch press.[31]

The Aroflex was modified in a second way, especially for Turkey. This country had bought (secure) Aroflex devices for communication with its NATO partners. For its internal communications Turkey had been using equipment of the French manufacturer Sagem.[32] These French devices used the one-time-pad (OTP) technology, which is perfect, in principle, as long as one does not re-use any keystream material. However, this is precisely what Turkey did: its keystream tapes were endlessly re-used in a circular manner, where, once a full round had been made, the tape continued a number of steps beyond the previous start position. This elementary mistake turned out to be fatal and made Turkish internal communications readable by many non-intended recipients (including TIVC).

When Turkey turned to Crypto AG to buy new equipment, a heated discussion erupted between the U.S. and Germany about whether this NATO partner should receive rigged devices or not – with Germany protecting Turkey's interests. The two (secret) owners of Crypto AG could not resolve the matter between them. The U.S. then gave up and opted for a different route: via the Dutch COMSEC authority NBV it approached Philips with the request to develop a special rigged version of Aroflex for Turkey.[33] Philips complied, as recently explained publicly by the Philips cryptographer involved.[34] This U.S.-instigated rigging happened via the Dutch COMSEC authority NBV, which is a separate organisation within the intelligence community, that kept the whole operation secret for several years from the Dutch code breakers at TIVC. As a result, critical questions were asked within Maximator about TIVC's role in the sudden appearance of unknown ciphertext emerging out of Turkey. TIVC was (also) clueless at first, but when it eventually found out about NBV's secret involvement together with the U.S., it was not amused.

3.3. Attacks in Paris and Berlin

The CIA and BND histories have been written by people who were not so closely involved in the cryptological aspects of the operation.[35] This might explain some inaccuracies and over-attributions in their accounts.

For instance, in 1991 an Iranian hit team assassinated the last prime minister under the Shah, Shapour Bakhtiar, at the time living in exile in Paris. The familiar story that the U.S. immediately provided France with proof of Iran's involvement from intercepted messages about the assassination, is repeated in 'Gedächtnisprotokoll', the internal BND document dated 11 December 2009, with the addition: '*Diese waren mit Geräten verschlüsselt, die von Bühlers Firma gekauft worden waren*', freely translated as: these message were enciphered with devices that had been bought from Bühler's enterprise, that is, from Crypto AG. This is then further discussed as grounds for Iran's growing distrust of Crypto AG and as proof of the irresponsible behaviour of the U.S. However,

a closely involved source in Dutch intelligence reports that the controversial Iranian messages were not at all encrypted with Crypto AG devices, but with a non-trivial manual cipher. Resulting cipher texts were intercepted and broken by TIVC, and apparently by many other SIGINT organisations as well. The fact that the Iranians learned that their (manually encrypted) communication had been compromised should not have surprised them at all and is not necessarily the reason for them to distrust Crypto AG.

In reaction to the La Belle discothèque bombing in West Berlin in 1986, 'Reagan appears to have jeopardized the Crypto operation after Libya was implicated' according to Greg Miller (based on the leaked CIA and BND reports).[36] However, Dutch intelligence sources from TIVC say that they never saw any encrypted communications coming out of Libya based on Crypto AG devices.[37] They suggest that the attack may have been carried out by a Libyan hit squad that used its own cipher – possibly a manual cipher too. However, TIVC never intercepted the 'La Belle' evidence itself, so it cannot fully exclude the possibility that Crypto AG technology was used in that affair. According to Faligot, the French did read the evidence,[38] so they (or the Americans) may be able to clarify the cryptographic nature of the communications.

4. Conclusions

In the slipstream of the recent revelations about the secret joint CIA and BND ownership of the company Crypto AG in the 1970 s and 1980s, this article reports on the European five-partner SIGINT alliance Maximator that began in the late 1970s. It discloses for the first time the name *Maximator* and provides documentary evidence. This European alliance has remained secret for almost fifty years, in contrast to its Anglo-Saxon Five-Eyes counterpart. The existence of this alliance gives a novel perspective on western SIGINT collaborations in the late twentieth century. This could be the starting point of a (historical) re-evaluation, in which the Five-Eyes partnership loses its prominence as the only environment for intense, long-term western SIGINT cooperation. Also, it may lead to a re-evaluation of geopolitical dependencies between various countries, based on access to (mechanisms for) diplomatic and military communications. The article explains and illustrates, with particular attention to the cryptographic details, how the five Maximator participants strengthened their effectiveness via the information about rigged cryptographic devices that their partner BND provided. Hopefully, a broader perspective on Maximator will emerge in the coming years, from more diverse sources.

Notes

1. See, for example, Aid and Wiebes, eds., *Secrets of Signals Intelligence*.
2. Internal CIA 'MINERVA: A History' document and internal BND documents listed in the references.
3. It extends the coverage provided in Wiebes, "Dutch SIGINT during the Cold War."
4. On this, see Faligot, "France, SIGINT and the Cold war," and Gehlen, *The Service*.
5. Produced by the Augustiner Brewery, the oldest independent brewery in Munich. See their website; https://www.augustiner-braeu.de/en/home.html.
6. To be historically precise, there were temporary names 'Ostsee' until 1977 and 'Alpenjäger' until 1979.
7. Norway stopped its (diplomatic) cryptanalytical efforts in 1965. See Jacobsen, "Scandinavia, SIGINT and the Cold War," 227–28.
8. As a result, Belgium was not 'protected' by the Maximator members and bought (weakened) Crypto AG equipment, as also reported in the leaked BND and CIA documents, so that its (Crypto AG based) communication was readable by both western five-member SIGINT alliances (Five-eyes and Maximator). Belgium used the Aroflex both for NATO and for internal communication, see Section 3.2. Belgium's cryptographic behaviour and discipline were problematic. For instance, at least once it compromised its own communications via a basic mistake in key management; also, it voluntarily replaced the (secure) Aroflex with the (insecure) Beroflex for its diplomatic communication, see Section 3.2 again. There is a stark contrast with Belgium's academic crypto community (esp. at KU Leuven) which operates at the highest international levels, producing global encryption and hashing standards AES and SHA-3 (adopted by the U.S. National Institute of Standards and Technology (NIST) in 2001 and in 2015).

9. Schmidt-Eenboom, "The Bundesnachrichtendienst, the Bundeswehr and SIGINT in the Cold War and After."
10. Wiebes, "Dutch SIGINT During the Cold War."
11. Faligot, "France, SIGINT and the Cold War."
12. This restriction of cryptanalytical discussions to bilateral meetings existed in the first few decades of Maximator's existence, but seems to have been relaxed later.
13. Meier and Staffelbach, "Fast Correlation Attacks on Stream Ciphers"; "Fast Correlation Attacks on Certain Stream Ciphers".
14. van Tuyll, "Design and Strength of a Feasible Electronic Ciphermachine from the 1970s."
15. See, for example, de Leeuw and Bergstra, eds., *The History of Information Security* for more historical information, and van Tuyll, "Design and Strength"; and Meier and Staffelbach, "Fast Correlation Attacks on Stream Ciphers"; "Fast Correlation Attacks on Certain Stream Ciphers", for technical specifics about attacking shift registers.
16. See YouTube, broadcast on 11 February 2020. https://www.youtube.com/watch?v=Q_9dfEX4SfU
17. Miller, "The intelligence coup of the century" and the documents cited at footnote 2, above.
18. Author's translation: 'These capabilities were not restricted to the U.S. and Germany; over the years countries like Denmark, France, Great Britain, Israel, the Netherlands, Sweden among others were included in those in the know.' A footnote in 'Einführung: Die Operation THESAURUS/RUBICON', Internal BND document, Nov. 2012, adds that those countries learned about the cryptographic details of the various devices, but not about the operation as such, that is, about the joint German-U.S. ownership and running of Crypto AG.
19. Aldrich, *GCHQ*, 442.
20. Speculatively: it may have been called *Fünfgruppe*, German for 'group of five'.
21. Also because the Maximator communications network (see Figure 2), was (partly) used by this second alliance too.
22. It was called *Wiskundig Centrum* (WKC) at first, but we shall use the later name TIVC that is also used in Wiebes, "Dutch SIGINT During the Cold War."
23. Venezuela used for a long time the CX52 M machine from Crypto AG.
24. For this reason these devices are often jointly called HC500. A similar device was the HC520, with the same encryption algorithm, which was not used by Argentina; its cryptographic keys were slightly different from HC550 and HC570 and were recognisable. For more information about these devices, see the online Crypto Museum; https://cryptomuseum.com/index.htm.
25. Aldrich, *GCHQ*, 389 & 402. See also, Wiebes, "Dutch SIGINT During the Cold War," 275.
26. It is unclear why the U.K. turned to the Europeans since its close American UKUSA partner knew in detail about the rigged Crypto AG algorithms. The reason might be that in the first few weeks of the war the Americans hesitated about choosing sides in the conflict. Greg Miller in the *Washington Post* writes: 'In 1982, the Reagan administration took advantage of Argentina's reliance on Crypto equipment, funneling intelligence to Britain during the two countries brief war over the Falkland Islands, according to the CIA history, which doesn't provide any detail on what kind of information was passed to London.' Miller, "The intelligence coup of the century". This suggests that the U.K. received decrypted intelligence products from the US, but not the method to decrypt itself. However, the BND author of 'Gedächtnisprotokoll', the internal BND document dated 11 December 2009, has no doubt that the U.K. got the decryption method from the U.S.: '*Die Briten hatten die Entzifferungs-Lösungen natürlich von den Amerikanern*'. A logical explanation might be that GCHQ asked *both* the Americans and the Europeans – that is, it asked both five-party sigint alliances – and that the Dutch were simply the first to respond.
27. MINERVA, a history. Internal CIA document, 2004.
28. Aldrich, *GCHQ*, 399.
29. Some of the mathematical details: solving the Beroflex involved finding a solution for one of 2^{24} systems of 150 binary linear equation with about 110 variables each. The well-known mathematical technique for finding such a solution is called Gaussian elimination. Each system of equations involved a matrix with 150 rows and 110 columns, which could be reduced via Gaussian elimination to a diagonal matrix of size 110×110. The specially developed chip could handle a 14×14 matrix. A sufficiently sized diagonal matrix of size 112 requires $36 = 8 + 7 + \ldots + 1$ of such chips. This set-up could solve a linear system in 150 clock cycles. With the chip's working speed of 1 Mhz the Beroflex could be solved in at most $150 * 2^{24}/10^6/60 \sim 42$ minutes.
30. MINERVA, a history. Internal CIA document, 2004.
31. In newspaper *De Volkskrant*, 20 February 2020.
32. Specifically, the CPP-ME model.
33. This route had been tried before in the Netherlands, for the pocket encryptor PX1000 that originally contained the strong encryption algorithm DES. The NSA paid Philips handsomely – tens of millions of dollars – to buy the rights and remaining stock of PX1000 devices from the manufacturer Text Lite and to start selling a new version of PX1000 with a more 'government friendly' algorithm provide by the NSA. This story has attracted quite some press attention in the Netherlands, for instance from the radio programme *Argos* (20 April 2019) and weekly magazine *De Groene* (7 August 2019). See also the Crypto Musuem website and Brücker, *Government intervention on consumer crypto hardware*.

34. Prof. dr. Cees Jansen in a Radio Interview, *Argos*, 15 February 2020; see also his own website https://www.ceesjansen.nl/en/.
35. With the possible exception of 'Einführung: Die Operation THESAURUS/RUBICON'.
36. Miller, "The intelligence coup of the century."
37. Recall that (HF and SHF) intercepts were shared within Maximator, so had any of the partners seen Crypto AG based ciphertext from Libya, the Dutch could have seen it too. What did get intercepted was traffic out of Libya encrypted via devices of the manufacturer Gretag.
38. Faligot, "France, SIGINT and the Cold War," 195.

Acknowledgements

Thanks are due to Huub Jaspers, investigative journalist for Dutch radio programme Argos, and Peter F. Müller, German freelance documentary filmmaker, for participating in joint research efforts. Thanks are also due to unnamed Dutch intelligence sources for kindly sharing information, explanations, and documents.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Bart Jacobs (1963) is a professor of computer security at Radboud University Nijmegen in the Netherlands since 2003. His work covers both the technical and the societal aspects of his field. He is often in the media and in parliament on topics like privacy, security and intelligence. He is member of an external expert board to the independent Review Committee on the Intelligence and Security Services (CTIVD) in The Netherlands and also member of the national Cyber Security Board.

Jacobs has published over 100 scientific articles. He is a member of the Academia Europea. For more details, see his personal webpage at the university: http://www.cs.ru.nl/~bart/

ORCID

Bart Jacobs http://orcid.org/0000-0002-0740-0336

Bibliography

Aid, M., and C. Wiebes, eds.. *Secrets of Signals Intelligence during the Cold War and Beyond*. Cass Studies in Intelligence, London, Portland, OR, 2001.

Aldrich, R. *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. London: HarperCollins, 2010.

Brücker, B. "Government Intervention on Consumer Crypto Hardware." Bachelor Thesis, Radboud University Nijmegen, 2014. https://www.cs.ru.nl/bachelors-theses/2014/Ben_Brucker___0413291___Government_intervention_on_consumer_crypto_hardware.pdf.

de Leeuw, K., and J. Bergstra, eds. *The History of Information Security*. Amsterdam: Elsevier, 2007.

Faligot, R. "France, SIGINT and the Cold War." *Intelligence and National Security* 16, no. 1 (2001): 177–208. doi: 10.1080/714002843.

Gehlen, R. *The Service: The Memoirs of General Reinhard Gehlen*. London: Collins, 1972.

Jacobsen, A. "Scandinavia, SIGINT and the Cold War." *Intelligence and National Security* 16, no. 1 (2001): 209–242. doi:10.1080/714002837.

Meier, W., and O. Staffelbach. "Fast Correlation Attacks on Stream Ciphers." In *Eurocrypt'88, Number 330 in Lect. Notes Comp.Sci*, edited by C. Günther, 301–314. Berlin: Springer, 1988. https://dblp.org/db/conf/eurocrypt/eurocrypt88.html

Meier, W., and O. Staffelbach. "Fast Correlation Attacks on Certain Stream Ciphers." *Journal of Cryptology* 1, no. 3 (1989): 159–176. doi:10.1007/BF02252874.

Miller, G. 2020. "The Intelligence Coup of the Century." *Washington Post*, February 11. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

Schmidt-Eenboom, E. "The Bundesnachrichtendienst, the Bundeswehr and SIGINT in the Cold War and After." *Intelligence and National Security* 16, no. 1 (2001): 129–176. doi:10.1080/714002841.

Undisclosed BND employee. 2009. "Gedächtnisprotokoll." *Internal BND document*, December 11.

Undisclosed BND employee. 2011. "MINERVA." *Internal BND document*, June.
Undisclosed BND employee. 2012. "Die Operation Thesaurus." *Internal BND document*, October.
Undisclosed ZfCh employee. 2012. "Einführung: Die Operation THESAURUS/ RUBICON." *Internal BND document*, November.
Unknown CIA Historian. 2004. "MINERVA, a History." *Internal CIA document*.
van Tuyll, J. 'Design and Strength of a Feasible Electronic Ciphermachine from the 1970s'. In B. Megyesi (ed.), HistoCrypt 2018: Int. Conf. on Historical Cryptology, pp. 153–158. Linköping Univ. Electronic Press, 2018. http://www.ep.liu.se/ecp/contents.asp?issue=149.
Wiebes, C. "Dutch SIGINT during the Cold War, 1945-94." *Intelligence and National Security* 16, no. 1 (2001): 243–284. doi:10.1080/714002820.