

Manuscript version: Author's Accepted Manuscript

The version presented in WRAP is the author's accepted manuscript and may differ from the published version or Version of Record.

Persistent WRAP URL:

<http://wrap.warwick.ac.uk/137156>

How to cite:

Please refer to published version for the most recent bibliographic citation information. If a published version is known of, the repository item page linked to above, will contain details on accessing it.

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

Please refer to the repository item page, publisher's statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk.

Operation Rubicon: Sixty Years of German-American success in signals intelligence

Richard J. Aldrich, Peter F. Müller, David Ridd and Erich Schmidt-Eenboom

Until June 2013, researchers were often in the dark about modern signals intelligence. Suddenly, Edward Snowden surprised the world by releasing a vast number of files on recent NSA and GCHQ activities, dating back to the early twenty-first century. Their volume was considerable and, together with other unauthorised releases, this material has kept academics and journalists busy puzzling over programmes like ‘Tempora’ and ‘Prism’ for years.¹ The Snowden files also place us in a curious position in terms of our overall knowledge of the history of signals intelligence or ‘sigint’. We probably know rather more about this esoteric activity in the early twenty-first century than we do about equivalent operations in the 1960s, 1970s or the 1980s. Meanwhile, the pace of formal declassification on sigint remains rather slow and so historians using official archival materials are still carefully piecing together the events of the 1950s. This scholarly work on the early Cold War is very impressive. Nevertheless, the late twentieth century remains a strange lacuna in the landscape of sigint.²

Understanding sigint in the latter decades of the last century is important because it constitutes a prelude to our present technological times.³ Periodically, fresh material emerges and provides new insights. In 2019, documentation was obtained in Europe that contributes more to our understanding of this fascinating period and that highlights the complex interaction between the United States, Germany, Switzerland and Sweden as key sigint partners during the second half of the twentieth century. These documents validate what many analysts and activists had long suspected about the relationship between corporations and western intelligence agencies, and also add fascinating detail that reshapes our understanding in surprising ways.⁴

The new material shows that during the 1950s, Boris Hagelin, the owner of one of the world’s largest cypher machine factory, Crypto AG, concluded a “Gentleman’s Agreement” with the famous American codebreaker William Friedman. He agreed to restrict the supply of his cryptographic devices around the world - and later weakened them - so that Washington could access their traffic. Eventually, the machines were designed by NSA engineers so that the encyphering was strong enough to fool purchasers into thinking their communications were secure, but weak enough to be read. In practice, this allowed a number of other advanced countries to read these machines more easily.

This operation, known first by the code name “Thesaurus” and later “Rubicon,” ranks among the most remarkable in the history of espionage – probably equal to the American triumph over “Magic” or Britain’s work against “Enigma” to defeat Axis wartime communications. Although the core countries in Operation Rubicon were Germany, the United States, Switzerland and Sweden, an outer ring of collaborators was required in order to control the flow of alternative machines from other manufacturers. Thus Britain, the Netherlands, France and Israel were also important to the wider project. Meanwhile, all states

with high-grade computing were secret beneficiaries of these operations and derived substantial flow of intelligence as a result.

Crypto AG was located near Zug in Switzerland. Perhaps 120 countries and also international organisations bought cypher machines from them, placing their faith in Swiss neutrality and scientific competence. By the 1970s, Crypto AG dominated the world market for encryption machines. Actually, between 1970 and 1993, this business was covertly controlled together by the CIA and the German secret service, the BND, often diverting the profits to other secret projects. As ZDF television's recent path-breaking documentary has demonstrated, Crypto AG's many customers paid huge sums, only to have their secrets stolen by a ring of the most technically advanced countries.⁵ As a result, during the 1970s and 1980s, a ring of some ten countries, probably including the Soviet Union, read approximately half of all "secret" communications traffic across the global south, with considerable impact upon diplomacy, political events and trade negotiations, not to mention wars and conflict.

The full history of Operation Rubicon is too complex to expound in anything other than a book-length study. However, herein, in this special section, three scholars who have reviewed the primary documentation obtained by ZDF's dogged investigation explore some of the most important themes. Melina Dobson asks what this means for our concept of intelligence power, and suggests that we have seriously underestimated Germany's importance in a landscape of sigint literature, a body of work that is too heavily weighted towards UKUSA and the Anglosphere.⁶ Sarah Mainwaring asks a related question in the American national context – have we misunderstood the nature of the CIA and overlooked its significance as a sigint actor? Jason Dymidiuk ponders the curiously unsecure nature of Operation Rubicon, reflecting on its resilient success, and the persistence of its core operatives, despite suffering repeated revelations. Bart Jacobs examines complex European sigint co-operation Maximator in the shadow of Rubicon and shows us that UKUSA was by no means the only game in town. Moreover, all four essays reflect on the importance of a national technical base – intelligence power in the late twentieth century was not just about agencies but also required manufacturing support and the leveraging of industrial contacts – through large companies like IBM, Racal, Phillips, Siemens and Motorola. The resulting technical lineage leading towards Microsoft, Facebook and Google is not hard to see.

How has the story of Rubicon emerged? As all the essays in this special section demonstrate, the manipulation of Crypto AG cypher machines has been known for a long time. Most spectacularly it was partly surfaced by Ronald Clark in 1977, and then more fully by James Bamford in 1983, who both sensed that there was a wider global narrative in the US sigint effort. Their main source was the papers of William Friedman, which were deposited at the Marshall Library in Lexington in 1969. Friedman was above all, a scientist and wanted recognition, hoping that the secrets of his friendship with Boris Hagelin and their work together would eventually come out. Accordingly, among the seventy-two boxes of his papers, were copies of his lifelong correspondence with Hagelin and references to something called the "Boris Project".⁷

Yet, as we shall see, these remarkable revelations did not dent the effectiveness of Operation Rubicon. Managers at the Crypto AG factory near Zug in Switzerland brazenly responded with a convincing counter-narrative. They dismissed Bamford's account as rumours designed to discourage countries in the global south benefitting from the secrecy provided by high-grade Swiss machines. However, in 1993, one of the company sales team, Hans Bühler, was arrested in Iran. After his release, Bühler's story attracted the attention of Scott Shane, a journalist working for *The Baltimore Sun*, a paper based close to NSA's

headquarters north of Washington DC. He continued to probe retired Crypto AG employees for further information. On 10 December 1995, he published a lengthy article adding much new detail.⁸

Even in 1995 the name of this activity – ‘Operation Rubicon’ – was still not publicly known. Indeed, it operated at such a high level of secrecy that, within the State Department, only the Secretary of State was cleared to know the internal dynamics of how it worked. Whilst many officials benefitted from the end product, the contours of the operation were tightly held. We only know about Rubicon because it was a product of intelligence collaboration or “liaison” between many advanced countries and therefore the secrecy net widened as the operation aged. Importantly, in September 1999, with Operation Rubicon in decline, but still active, veterans of the American and German secret services gathered for a historical conference at Teufelsberg in Berlin. Some of the attendees, brimming with pride at the amount of intelligence their joint operation had produced, decided to create a final report.

By 2004, a 96-page historical document had been written by the CIA. Borrowing the CIA’s codename for Crypto AG, it was entitled ‘Minerva’. Unusually, this history was not undertaken by the CIA’s History Staff, but by others. Moreover, the ‘Minerva’ document was in fact a summary of a larger and highly classified three-volume study of the same subject. The 96-page ‘Minerva’ summary was designed to be given to the BND as an official history and joint memorialisation. In turn, and because of inaccuracies they perceived in the American narrative, the German BND responded with their own oral history made up of contributions from senior intelligence officers who had overseen or staffed the programme.

Later, these materials surfaced during a lengthy programme of research by the German broadcasting company ZDF, who began making a series about the BND, an intelligence service which undertakes both human and technical espionage.⁹ During the creation of this series, the 96-page ‘Minerva’ document emerged, together with the German commentaries, triggering a new wave of research by veteran journalists Peter F. Müller, Ulrich Stoll and David Ridd, in conjunction with the leading German intelligence specialist Erich Schmidt-Eenboom. Travelling the world, they conducted many interviews to cross-check the material, including access to many distinguished veterans. Subsequently they collaborated with Greg Miller at *The Washington Post* to further probe the American side of the story. Nicole Vögle and Fiona Enderes from Swiss television *SRF* together with Huub Jaspers from the Dutch radio programme *Argos* also contributed.¹⁰ Eventually, many senior officials, including a former Director of the NSA, Bobby Ray Inman, together with Bernd Schmidbauer the minister responsible for the BND under Helmut Kohl’s chancellorship, confirmed the accuracy of the material. Meanwhile NSA has finally begun releasing more of the Friedman papers.¹¹

The full story of Operation Rubicon has not yet been unravelled. Its narrative interweaves with the complex cryptographic histories of more than half the countries in the world, and indeed much of our recent technical and industrial history. In a sense it is emblematic of our times. For now, the role of key partners like Sweden and Switzerland, which also constitute sigint ‘great powers’, remains largely mysterious.¹² Although the researchers writing here have been generously permitted to access the materials gathered by ZDF, caution must be exercised, since some of the papers are celebratory and even self-congratulatory.

Operation Rubicon was vast in scale and its foundations, built on a complex network of long-term personal relationships, some of which even pre-dated the Second World War. It

is clear, however, it has the potential to alter some of our existing assumptions about the Cold War. The task of excavating its full extent will keep intelligence scholars busy for many years to come.

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 – Centenary Edition*. London: HarperCollins, 2019.

Aldrich, R. and J. Kasuku. "Escaping from American Intelligence: Culture Ethnocentrism and the Anglosphere", *International Affairs* 88, no. 5 (2012): 1009-1028. www.jstor.org/stable/23325014.

BBC News. 2014. "Snowden NSA: Germany to investigate Merkel 'phone tap'." June 14. <https://www.bbc.co.uk/news/world-europe-27695634>.

Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency*. New York: Houghton Mifflin Company, 2009.

Berridge, G. R., and John W. Young. 'What is "a Great Power"?' *Political Studies* 36, No.2 (1988): 224-234.

BND, internal document. 2009. BND, 13-14 August.

Clark, Ronald, *The Man Who Broke Purple: The Life of the Worlds Greatest Cryptologist Colonel William F. Friedman*. London: Weidenfeld and Nicolson, 1977.

Corera, Gordon. *Intercept: The secret history of computers and spies*. London: Hachette UK, 2015.

Davies, P. and K. Gustafson. *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere*. Washington DC: Georgetown University Press, 2013.

Easter, David. 'Spying on Nasser: British signals intelligence in Middle East crises and conflicts, 1956–67.' *Intelligence and National Security* 28, no.6 (2013): 824-844.

Herman, Michael. *Intelligence power in peace and war*. Cambridge: Cambridge University Press, 1996.

Jacobs, Bart. 'Maximator: European signals intelligence cooperation, from a Dutch perspective.' (2020). doi:[10.1080/02684527.2020.1743538](https://doi.org/10.1080/02684527.2020.1743538).

Karatzogianni, Athina, and Martin Gak. 'Hack or be hacked: the quasi-totalitarianism of global trusted networks.' *New Formations* 84.84-85 (2015): 130-147.

Miller, G., 'The Intelligence Coup of the Century.' *Washington Post*, 11 February 2020. <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.

Shane, Scott & Tom Bowman, 'Rigging The Game', *Baltimore Sun*, December 10, 1995.

Wark, Wesley. 'The road to CANUSA: how Canadian signals intelligence won its independence and helped create the Five Eyes.' *Intelligence and National Security* 35. no.1 (2020): 20-34.

ZDF, Operation RUBIKON, 18 March 2020, <https://www.zdf.de/dokumentation/zdfinfo-doku/operation-rubikon--100.html>.

¹ BBC News. 2014. "Snowden NSA"

² Important examples include Easter, 'Spying on Nasser'; Wark, 'The road to CANUSA'.

³ This subject has most recently been probed by Aid and Wiebes, (eds.). *Secrets of Signals Intelligence during the Cold War*; Aid, *Secret Sentry*, and Aldrich, *GCHQ*.

⁴ Karatzogianni and Gak. 'Hack or be hacked'.

⁵ ZDF, 'Operation RUBIKON', 2020.

⁶ Davies and Gustafson (eds.) *Intelligence Elsewhere*; Aldrich and Kasuku, 'Escaping from American Intelligence'.

⁷ Clark, *Man Who Broke Purple*; Bamford, *Puzzle Palace*.

⁸ Shane & Bowman, 'Rigging the Game'.

⁹ Schmidt-Eenboom, 'The Bundesnachrichtendienst'.

¹⁰ Miller, 'The Intelligence Coup of the Century'.

¹¹ Their importance was explained in Gordon Corera's fascinating and well-documented book *Intercept*.

¹² Berridge & Young. 'What is "a Great Power"?'; Herman, *Intelligence power in peace and war*.