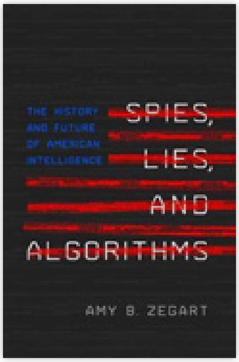
BOOKS



Spies, Lies, and Algorithms

The History and Future of American Intelligence
By Amy B. Zegart
Princeton (Princeton University Press) 2022
424 pages
ISBN 9780691147130
€30

There is certainly no shortage of spytainment, the term used to refer to espionage-themed entertainment. It features in books, films and television series, including *Homeland, CSI, 24*, and characters such as Jason Bourne, Jack Ryan and, of course, James Bond. However, according to Amy Zegart, while spytainment is everywhere, spy facts are scarce. Public knowledge about the why and how of intelligence services is very limited, not just because these services themselves are by nature secret or secretive. There is also relatively little attention given to intelligence work in academia, especially in international relations and in the broader political sciences. In her second chapter, Zegart, affiliated with Stanford University, explains clearly why such a lack of public knowledge about intelligence is problematic. If the only source of information is spytainment, the public gets a distorted picture of the intelligence world. Her own surveys show that spytainment fans attribute more power and capabilities to intelligence services than they actually possess, are more in favour of torturing terrorist suspects and estimate that there is less supervision than there is in reality. This can feed conspiracy theories, complicate debate on surveillance and spread misconceptions about torture. After all, the latter is both unethical and ineffective. The lack of knowledge carries through to the political and administrative level, with Zegart claiming that there are more Congress members with knowledge of milk powder than knowledge of intelligence services. The dean of West Point, Brigadier General Patrick Finnegan, was once so concerned that the series *24* glorified the torture of terrorist suspects among cadets that he visited the film set to ask whether they could also make an episode where torture had the opposite effect to what was intended. When he appeared on set in uniform with this request, people thought he was an actor.

18 intelligence services

The misconceptions about intelligence are the prelude to Zegart's book *Spies, Lies, and Algorithms*, an ambitious work aimed at providing a thorough background on intelligence and espionage. As a political scientist, Zegart has been investigating US intelligence services for thirty years. She previously wrote the book *Spying Blind. The CIA, the FBI, and the Origins of 9/11*. As she herself states, she does not inhabit the intelligence world (she has never worked for a service), but is a visitor. As an outsider – who, in addition to literature research, has spoken with many intelligence service employees – she has a fresh view on this rather closed world. On the one hand, she understands the challenges facing services and the high expectations they have to meet. Intelligence services must, for instance, generate high-quality intelligence, anticipate international developments and events in good time (preferably predict these), and do all of this without infringing on the privacy of others. James Clapper, director at the time of the US intelligence community (DNI), once referred to this as the problem of 'immaculate collection'. On the other hand, Zegart does not shy away from speaking out when it comes to the failure of the services, in terms of analytical mistakes and organisational misconduct alike. Her book is deliberately broad in scope – the subtitle is 'the history and future of American intelligence'. This is a huge field of research. The US now counts 18 intelligence services (but an organisation only counts if it has a three-letter acronym), more than 100,000 employees, some 4 million 'clients' who have security clearance, and all for a price tag of $85 billion per year. In short, more than the GDP of a considerable number of countries.

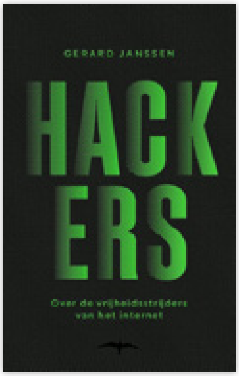
Pitfalls in the thinking process

The core of the book is made up of four chapters: a historical background of American intelligence; the principles of intelligence work (knowns and unknowns), why analysis is so difficult, and covert action. All the chapters include tables and text blocks that elaborate on certain cases. The historical context is original because Zegart goes back as far as the US War of Independence, in which George Washington managed, partly through espionage, ruses and deceit, to get the upper hand over the English, who are, after all, known as masters of the genre. Some examples from the Korean War are also well described. For example, General Douglas MacArthur was convinced that if China were to become involved in the war, its soldiers would have no chance whatsoever against the well-trained American soldiers. Things took a different turn, however. It brings to mind Russian President Putin's expectation at the beginning of 2022 that Ukraine would be under his control within a matter of days. Incidentally, this conflict is not described in the book; it was already at the printer at the time of the invasion. The chapter on analysis is also very worthwhile and describes various pitfalls in the thinking process (such as cognitive biases). Each chapter includes well-described case studies. From FBI mole Robert Hanssen, to Saddam Hussein's non-existent weapons of mass destruction and the hunt for Osama bin Laden; Zegart describes it all in beautiful detail.

Digital themes

A small point of criticism is the rather meagre discussion of the subject of cyber espionage. The word 'algorithm' in the title is seldom revisited in the book. This may be unavoidable given the broad focus of the work. The chapter on open-source intelligence focuses mainly on nuclear proliferation, but could just as well have devoted more attention to Bellingcat and algorithms, which have proved so effective in exposing Russian intelligence officers. The last chapter rushes headlong through the topics of online disinformation and offensive and defensive cyber operations. This deserved an extra chapter, with more conceptual distinction between the complicated digital themes. Regardless, Zegart's latest work certainly deserves a place on the bookshelf. For those who have had some introduction to intelligence studies, the work offers a fresh and broad perspective, with particularly the chapter on public knowledge and perception and the chapter on the US supervisory system adding new data and insights to the existing literature. The book is also a gold mine of source references. The text takes up some 275 pages, but Zegart also provides about one hundred pages in end notes and a short bibliography. Nonetheless the book will be most useful to people who are interested in intelligence but who do not yet have an overview of or grip on the field. In short, anyone who does not know the distinction between a case officer (or operator) and a source or an agent is advised to speedily acquire this book. *Spies, Lies, and Algorithms* will undoubtedly also appeal to fans of spytainment, because even though it has been written from an academic perspective, the interesting anecdotes, well-written stories and fluent writing style make the book especially entertaining.

Dr Sergei Boeke, Political Adviser at JSEC



Hackers

The internet's freedom fighters
By Gerard Janssen
Amsterdam (Thomas Rap) 2022
304 pages
ISBN 9789400408371
€22.99
Currently only available in Dutch

Hackers are often portrayed stereotypically: hoodies, a dark room, a screen with incomprehensible lines of computer code. Over the past several years author and journalist Gerard Janssen, has immersed himself in this mysterious world, with which he, like most readers probably, was previously unfamiliar. The book *Hackers* is the result of his quest. Breaking into a computer system is called hacking. Hacking is often done with malicious intent, but it can also be done to test a system for security. Janssen's book is about who these hackers actually are. It is not an analysis of how hacking works from a technical standpoint, what the impact of this is or how to take action against it. Janssen does write about that, but with the intention of explaining how a hacker thinks and operates. Janssen's quest starts from journalistic necessity: he must have facts and sound sources. But, he admits himself, it is also a world that fascinates him: a Marvel Comics world with people with 'online superpowers'. He did not need to look far afield for some leads because the Netherlands proves to have both a capable hacking community and a great deal of IT knowledge and experience to protect against hacking. For example, it was a Dutch person who notified the White House of the poor security of then president Trump's Twitter account and we have all heard of Fox-IT, which shows up in the media to give an explanation every time another major hacking incident occurs.

Guardians and malefactors

Hacking started with good intentions by curious students in the 1950s who had their computers play games with each other and magically caused messages to appear on each other's screens. In order to do so, they had to understand the functioning of the system of digital pathways of the computer, the operating system and application software. And, decades later, how communications are routed via the internet. The idea was to help people and technology, for example by detecting vulnerabilities that pose a risk to safe use of the internet and everything that is connected to or dependent on it. These hackers, as they are now called, see themselves as the guardians of the free internet, which they consider to be the 'last great bastion of freedom of thought, ideas and expression'. They observed that governments and big business want to keep control and 'always (opt for) functionality over safety (of the user)'.

But soon a group of hackers arose who use their knowledge to steal and exploit information for their own gain. The culture of ethical hacking, denoting the difference between those with good intentions and those with malicious intentions, is entirely alien to them. They have taken the path of spreading malicious viruses, using phishing techniques, launching DDOS attacks et cetera. This is what the author describes as the criminal side of hacking, which is particularly rampant in the Russian Federation. It is therefore certainly appropriate that Janssen quotes the Netherlands Public Prosecution Service on the criminal nature of hacking. He also mentions the existence of hackers with political activist objectives.

Janssen gradually penetrates further into the world of hackers on his quest. There are descriptions of all kinds of special meetings, often in places where hackers feel the safest and most comfortable: their *hackerspaces*, or during major hacking gatherings at home and abroad. The world of hackers is really not only to be found 'underground'. When he succeeds in gaining their trust, the hackers provide Janssen with information, albeit sparsely, about what they are capable of: how they are able to break into the IT systems of governments, companies and organisations, what kind of information they find and what they could do with that. But also how nonchalant or even hostile the reaction is if this kind of security leak is reported. For the rest, Janssen is careful not to get involved in the criminal parts of this world himself. What he learns about this comes second-hand from hackers and security experts.

Personal traits and qualities

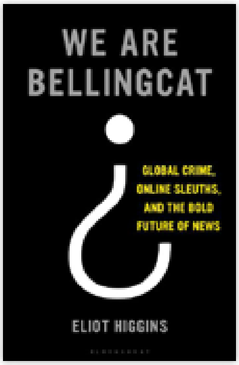
The conversations and meetings also provide Janssen with the information that allows him to tell more about the hackers themselves.

Janssen devotes ample attention to the personal traits and qualities of the people he meets. It is a sobering story about what starts as an innocent challenge – which comes with being young and knowing a lot about computers – and often ends up leading to an isolated and distrustful existence. It is a closed world. The outside world does not trust them, they do not trust the outside world. Conspiracy thinking is not alien to hackers. Some are sometimes literally constantly on the run. The hacker environment remains mysterious, with its own rituals and etiquette. Nor does the 'nerdy' image, which hackers seem to be happy to confirm, go unmentioned. Janssen does his best to place this alongside positive qualities, such as mutual tolerance, idealism and willingness to help each other and – on a personal level – their perseverance and inventiveness; they are intelligent and critical, according to him. However, those positive traits and the fact that many hackers turn out to have ordinary and responsible jobs in everyday life, often precisely in the IT world, do not allow this book to overturn the generally negative image that exists of hackers.

Janssen leaned heavily on the willingness of hackers to share knowledge and information with him for the writing of this book. A paradoxical situation: the author who wants transparency and the conversation partners who prefer to remain hidden. This tension is noticeable when reading this book. Not everything is said and not everything was written down, Janssen admits.

Janssen has written an entertaining book that certainly holds the reader's interest. He seems to capture the atmosphere of the hackers' world well, including by using colourful hacker jargon. In order to be able to place these exotic terms, the author has included, very helpfully, an extensive explanatory glossary. For the lay person who wants to know more about hackers than just the usual stereotypes and who wants to know how widely hacking is applied, this book is certainly worth a read.

Lieutenant Colonel Jan-Leendert Voetelink



We are Bellingcat

Global crime, online sleuths, and the bold future of news
By Eliot Higgins
Amsterdam (Spectrum) 2022
272 pages
ISBN 9781526615732
€23.99

In 1979, Italian historian Carlo Ginzburg wrote an article on a new form of scientific thinking at the end of the nineteenth century.[1] In it, he discusses a series of articles from 1874-1876 by Italian art historian Giovanni Morelli. In these articles Morelli attacked the practice at the time of attributing paintings. European museums were allegedly full of paintings attributed to the wrong artists. The so-called art experts, according to Morelli, went about it the wrong way. Specifically, they focused on the most eye-catching aspects of paintings, such as the smiles that Leonardo da Vinci often gave his portraits. Elements that were easy to fake, Morelli argued, not least because those very pieces of art were taught in certain schools. For that very reason, it was important to study the 'most negligible details': earlobes, nails and the shape of fingers and toes.[2] Not entirely coincidentally, Ginzburg argues, we see the same kind of attention to detail in Arthur Conan Doyle's books about Sherlock Holmes. Holmes also explicitly focuses on the smallest details that everyone else overlooks, thus going on to solve the most complex crimes. Ginzburg sees a new scientific paradigm in this: the 'paradigm of the trace', with an eye for what is in the background and not in the foreground. You will have to focus on the 'infinitesimal', Ginzburg says: only the marginal, the details – the fingernail or discarded match – allows the observant observer to penetrate to a deeper reality.[3]

Bellingcat

Eliot Higgins, founder of the open-source platform Bellingcat, is a bit like Morelli. In his book *We are Bellingcat. Global crime, online sleuths, and the bold future of news,* Higgins outlines the history of this group of digital civilian detectives and journalists. Like Morelli – who tried his method and managed to attribute a number of high-profile paintings to other artists – Higgins is keen to show what painstaking online research can achieve. And not without reason: Bellingcat now has an impressive portfolio – and this book is also best read as a portfolio. It consists mainly of summaries of the course and results of Bellingcat's digital sleuthing during the Arab Spring, the Syrian Civil War, the MH17 investigation, far-right violence in the United States, Islamic State executions, violent crimes in Libya and the murder of Sergei Skripal. The common thread – and core idea of Bellingcat – in these investigations is that the truth is hiding in the details. Ginzburg could not have wished for a nicer counterpart to the paradigm of the trace, even though Bellingcat puts *digital* traces at the centre. During the Arab Spring in 2011, Higgins noted that many journalists were using footage of dubious origin, mostly from involved parties. Many photos and videos that served as evidence were misinterpreted as a result. He set out to date and geolocate photo and video footage that had been presented to the world via social media or otherwise. The MH17 investigation and the murder of Skripal are perhaps the most spectacular examples.

[1] Carlo Ginzburg,'Clues. Roots of a Scientific Paradigm', Theory and Society 7 (1979) (3) 273-288.
[2] Ginzburg, 'Clues', 273-274.
[3] Ginzburg, 'Clues', 280.

Is Bellingcat thereby acting as a 'secret service for ordinary people' (p. 20)? There is no doubt that Bellingcat conducts admirable as well as relevant investigation. Tracing and verifying online material for truth-telling purposes requires systematic, meticulous and time-consuming work from which there is much to learn. Especially regarding attribution issues – digital or otherwise – which is in the purview of intelligence and security services. But the objectives, activities and handling of data acquired by these services, from public sources or otherwise, are broader and different from Bellingcat's, such that the characterisation 'secret service' misses the mark. Intelligence and security services in a democracy serve the security of state and society. Independence, objectivity and speaking truth to power is the common adage. Yet their work is not outside the political realm. In the event of a political decision to undertake a military mission or combat jihadist terrorism, military and civilian services cannot avoid reporting on it regularly. Services can maintain professional distance but are not separate from politics. In contrast, Higgins claims to have nothing to do with 'political agendas' (p. 34). However, one could consider Bellingcat's choice of topics as a political act: why look at Rupert Murdoch's eavesdropping scandal? And the mere fact that Bellingcat cooperates with police forces means taking a stand against the Russian and Syrian states, for example. And the 'declaration of war' on the 'counterfactual community' is not apolitical either, of course.

A second important element of Bellingcat's identity concerns its distance from the subject. At several points in the book, Higgins stresses that the lack of language and cultural knowledge actually allows Bellingcat to look at the details. For intelligence and security services, the Bellingcat method of digital digging may be important, but without military experts, linguists, historians, or technical specialists, all that can be determined is where and when a photo or video was taken. The meaning of what can be seen, or what has been said or done requires active interpretation based on relevant – and thus context-related – knowledge and skills.

This brings us to a final difference. In addition to attribution activities for events that are in the past – either to identify perpetrators or draw lessons – secret services are there to give early and strategic warnings. They must warn about national security risks to enable other players to take action. This presupposes that they make statements about possible, future actions of states, groups and individuals. In doing so, it is not enough to be transparent, like Bellingcat; after all, the facts do not speak for themselves as they do for the digital forensic tracking in which Bellingcat engages. On the contrary, the context in which statements and actions are to be understood plays a major role in the interpretation of a threat.

Secret service or Sherlock Holmes?

Higgins, in his enthusiasm for Bellingcat's online research, can be blamed for what critics accused Morelli of a century and a half ago: positivism – understood for convenience as the unshakable belief in the irrefutable existence of (observational) facts. According to Ginzburg, this is fundamental to the paradigm of the trace, which calls for attention to the infinitesimal and marginal. Therein, after all, lie the facts that provide access to a deeper truth. Higgins believes the same thing. The facts are there for the taking in the public domain; just hidden in the details, like the metadata of a file, a minaret in the background, or a faint plume of smoke that is in view for just a second. That, however, does not make Bellingcat a secret service for ordinary people, rather a public Sherlock Holmes – a detective engaged in fact-finding in the context of investigating perpetrators. This does not diminish the importance of this open source research. An independent organisation which fact-checks and is thorough and innovative in doing so is an important ally for ordinary citizens, especially in a time of information overload and disinformation.

Dr C.W. Hijzen, research fellow at the Institute of Security and Global Affairs of Leiden University
Dr A. Claver, Ministry of Defence