

Krzysztof SURDYK<sup>1</sup>  
Poland

## INTELLIGENCE IN THE FACE OF THE TECHNOLOGICAL CHALLENGES OF THE 21st CENTURY

**Abstract:** *This article presents the changes that have occurred and are occurring in foreign intelligence due to the ongoing development of new technologies. It emphasizes the importance of human intelligence, which remains crucial for national security and has been enhanced by new technological solutions. Based on proposals developed for the U.S. Intelligence Community, it highlights a shift in the approach to analytical matters in intelligence, emphasizing a focus on the analysis of big data sets. Due to the development of digital databases and internet connectivity, it highlights the increased opportunities for intelligence acquisition and the shift of some intelligence activities to cyberspace, not forgetting the threats this poses. It also presents the threats that may arise for intelligence communications due to the emergence of quantum computers and the ability to decrypt previously secure intelligence transmissions. It highlights the importance of new technological and organizational solutions in technical intelligence (SIGINT, IMINT) and open-source intelligence (OSINT). Finally, it analyzes the possibilities of creating agent-based artificial intelligence.*

**Keywords:** *new technologies, Humint, SIGINT, IMINT, OSINT, Pervasive Technical Surveillance.*

### Introduction

New technologies of the 21st century are sweeping across all areas of human activity. We often fail to notice the changes we experience in our lives, taking them for granted, and only when we look back on the past years do we realize the enormity of these changes. Intelligence, a crucial element of every country's ex-

<sup>1</sup> Krzysztof Surdyk, PhD, The Józef Gołuchowski University of Applied Sciences

ternal security, is also experiencing these changes, although we traditionally associate intelligence activities with recruiting agents who steal secret documents from the safes of hostile states. Meanwhile, new technologies are revolutionizing these activities at every stage. For those less versed in intelligence operations, it's worth reminding that the individual stages of intelligence work stem from the so-called intelligence cycle. Classically, the intelligence cycle is divided into five components:

- planning and tasking;
- data collection – acquisition;
- intelligence processing – transformation into intelligence information;
- analysis and synthesis of intelligence information – transforming it into knowledge (reports, conclusions, and recommendations);
- distribution (delivering it to interested recipients).

The implementation of the intelligence cycle determines the substantive components of each intelligence structure. In addition to management, this structure comprises two basic functional divisions: the intelligence collection division and the analytical and information division. Another important component of intelligence, not directly derived from the intelligence cycle, is the operational and technical support division. Technological innovations have a significant impact on the functioning of individual intelligence functional divisions. Thus, in the intelligence collection division, new solutions are emerging in previously used intelligence collection methods, such as Humint<sup>2</sup>, OSINT<sup>3</sup>, SIGINT<sup>4</sup>, and IMINT<sup>5</sup>, revolutionizing the acquisition of this data, as well as addressing problems arising from the technological development of counterintelligence techniques. Above all, however, intelligence gathering has significantly shifted to cyberspace, where both hacking techniques for database intrusion and sophisticated attacks on the IT networks of potential adversaries have developed. The internet and connected devices are ubiquitous, offering intelligence agencies numerous opportunities for surveillance, provocation, and covert operations. Organizations monitoring and operating on

<sup>2</sup> Humint (Human Intelligence) – a category of intelligence activities involving the acquisition/obtaining of information provided by personal sources.

<sup>3</sup> OSINT (Open-Source Intelligence) is a category of intelligence involving the collection of information from publicly available sources. It is used in both state and economic intelligence.

<sup>4</sup> SIGINT (Signals Intelligence) – a type of intelligence (reconnaissance) activity conducted in an electromagnetic radiation environment, including in telecommunications and information technology. Also known as electromagnetic, electronic, radio, and other intelligence.

<sup>5</sup> IMINT – (Imagery Intelligence) – image intelligence or image reconnaissance, enabling the generation of data based on images from photographs, radars, electro-optical devices operating in infrared and thermal imaging, and other devices.

the internet are often private companies, not government agencies. Over a billion cameras installed worldwide are part of a growing network of technological surveillance, complicating the lives of intelligence officers and the agents they recruit. Intelligence agencies spend their time acquiring secrets, protecting their own, and engaging in covert activities that other branches of government would rather not engage in, such as gaining political and economic influence, maintaining secret contacts with terrorist groups, thwarting conspiracies, or secretly eliminating enemies. For over a century, technology has been an integral part of this process. As the world transitioned from „communicating by courier to telegraphs and radio, intelligence became mechanized and industrialized”, wrote Michael Warner, a former CIA<sup>6</sup> historian. Intelligence became one of the main consumers of the latest technology. The advent of spy satellites exposed the Earth’s surface. New gadgets, such as miniature transistors and secret inks from the emerging plastics industry have transformed the way human intelligence operates. Meanwhile, the analytical and information department is primarily observing a shift from traditional analytical processes to a data-centric approach. This situation has been forced by the enormous volume of data (Big Data) that intelligence analysts must process and analyze. Technologies also have a huge impact on the operational and technical security of intelligence, although this impact is highly variable. In some areas of intelligence operations security, such as legalization<sup>7</sup>, serious problems arise. Due to the yearly improvement of biometric security, the production of operational documents is becoming increasingly difficult. In other areas, such as communications with agents, modern computer technologies are creating new, previously unavailable communication possibilities, suffice it to mention computer steganography<sup>8</sup> or SRAC<sup>9</sup>. At the same time, however, threats are emerging, including the hacking of computer intelligence communications by counterintelligence agencies, as well as the prospects of widespread introduction of quantum computers, which may result in the current encryption methods commonly used in intelligence services proving insufficient.

---

<sup>6</sup> Michael Warner, a former historian at the Central Intelligence Agency (CIA), is currently a historian at the United States Cyber Command. He previously worked as a historian for the CIA and the Office of the Director of National Intelligence. He is an author and lecturer on intelligence history, intelligence theory, and intelligence reform.

<sup>7</sup> Legalization – the right to use documents that make it impossible to determine the data identifying an intelligence officer and the means he uses when performing official tasks (so-called legalization documents) in the case of performing operational and reconnaissance activities.

<sup>8</sup> Steganography (Greek: *στεγανός*, *steganos*, „hidden, protected”, and *γράφειν*, *graphein*, „to write”) is the science of communicating in such a way that the presence of a message cannot be detected. Unlike cryptography (where the presence of a message is not denied, but its content is secret), steganography attempts to conceal the fact that communication is taking place. Steganographic techniques are also used to mark digital data.

<sup>9</sup> SRAC (Short-Range Agent Communication). More details later in the article.

The above observations demonstrate that in a world where the threat landscape to national security is constantly evolving, intelligence operations must also evolve. The need for change in intelligence operations is best demonstrated by the U.S. Intelligence Community (IC) Information Environment Vision, published in June 2024, the so-called „Information Technology Roadmap”<sup>10</sup>, which expresses the urgent need for IC transformation, drawing attention to the fact that the current strategic intelligence environment, encompassing both state and non-state actors, is radically different from that of September 2001. This evolving, dynamic environment requires intelligence, and above all its IT infrastructure, not only to keep pace with ongoing changes but also to provide it with a strategic advantage. The aforementioned „Roadmap” sets ambitious goals. It identifies five key areas, each aimed at improving intelligence operations through a comprehensive IT strategy. These areas include:

1. Strengthening intelligence operations by creating a solid and resilient digital foundation;
2. Enabling the implementation of intelligence activities through reliable digital security (cybersecurity);
3. Ensuring the implementation of intelligence activities through modern intelligence practices and partnerships with allies;
4. Improving the implementation of intelligence activities through so-called data focus;
5. Accelerating the implementation of intelligence activities through advanced technologies and highly qualified employees.

There is no doubt that open data sources (to which commercial companies also have access) are currently gaining in importance. However, this does not mean that intelligence agencies can be dismantled and rely solely on publicly available data. Just because such data can answer many questions that previously required covert intelligence operations does not mean they can answer all of them. The second problem lies in assessing the credibility of the data. Agencies verify its credibility before beginning intelligence analysis. Confirming it with several different open sources is not always enough. In many cases, the value of open-source data must be confirmed by data obtained from classified sources. The third problem concerns the legal and ethical issues raised by the data contest. For Chinese intelligence services, a key part of their strategic competition with the West revolves around data. According to British intelligence, over the past decade,

---

<sup>10</sup> *Vision for the IC Information Environment An Information Technology Roadmap*, <<https://www.dni.gov/files/documents/CIO/IC-IT-Roadmap-Vision-For-the-IC-Info-Environment-May2024.pdf>> (30.05.2024).

Chinese intelligence has acquired vast amounts of data, including US government personnel files, UK election data, Indian immigration data, South Korean phone records, and Taiwanese road maps. Much of this is traditionally collected intelligence, some of which is intended to enable China to catch Western spies.

Western agencies are limited in their ability to acquire data domestically, although they can and do collect mass personal data from abroad. Emily Harding, a former CIA analyst, argues that it is „difficult, if not impossible to identify and cleanse data about Americans from large datasets, a legal requirement. Consequently, American agencies lag behind private sector organizations that don't have such restrictions”<sup>11</sup>.

### **A New Approach to Data Processing and Analysis<sup>12</sup>**

The vision of data centralization requires certain transformational actions in the field of intelligence processing and analysis. This involves moving away from the paradigm of operating in isolated databases toward analyses conducted in an integrated, flexible, and efficient data environment. This transformation is crucial to ensuring analysts can quickly and precisely generate useful insights and conclusions, thus streamlining the entire intelligence process. One of the most important aspects of the U.S. Intelligence Community's Information Technology Roadmap mentioned above is the fourth priority area, which is improving intelligence execution by focusing on data.

This area emphasizes the importance of effective data management and its secure use. To achieve the intended focus on data, especially large data sets, the IT system must consistently manage data at every stage of its lifecycle. Such operation of the IT system would not be possible without comprehensive data management planning. Planning allows for the adaptation of data lifecycle management to the IT architecture critical to a given intelligence mission. Whether collecting data from specialized sensors or video recordings in a remote location, or drawing conclusions from this data in an isolated facility, such planning allows for the widespread introduction of advanced applied analytics and AI into intelligence. Organizationally, this approach also allows for the creation of a Data Service common to national intelligence institutions. This kind of service is currently planned within the U.S. Intelligence Community.

Implementation of a Data-Centric Architecture. Evaluating data as a strategic enabler of the intelligence process requires the establishment of common data standards, models, services, and digital policies across the institutions using it. This is essential to ensure that everyone processes critical information consistently, and that every object using this data is appropriately protected and shared.

<sup>11</sup> J. Shashank, How private intelligence companies became the new spymasters, <<https://engelsbergideas.com/essays/private-intelligence/>> (24.09.2024).

<sup>12</sup> E. Larina, V. Ovchinsky, *How Intelligence Has Changed in the World of Technology*, <[https://zavtra.ru/blogs/kak\\_izmenilas\\_razvedka\\_v\\_mire\\_tehnologij](https://zavtra.ru/blogs/kak_izmenilas_razvedka_v_mire_tehnologij)> (08.07.2024).

Establishing common standards allows for the creation of a decentralized data ecosystem, ensuring seamless data sharing and facilitating the implementation of advanced artificial intelligence and machine learning (AI/ML) capabilities. Ultimately, an IT system architecture built on these principles will streamline data sharing and collaboration within intelligence departments, national intelligence communities, and with external partners.

Transitioning from classified data to data-centric enclaves. Classified data within the intelligence analysis department is often isolated, which in practice makes it difficult for analysts to access and utilize information. By moving to data-centric enclaves, the intelligence analysis department can break down these barriers, enabling authorized users to search and access relevant data more efficiently and effectively. Broadly speaking, this is about shifting intelligence analysis from traditional analytical processes to a data-centric approach. For example, the aforementioned „Roadmap” report makes recommendations to the U.S. Intelligence Community in this regard, stating, among other things, that „timely, accurate, and informed reasoning is key to achieving better intelligence mission outcomes, and the Intelligence Community should move from an organization- and system-centric paradigm to a data-centric paradigm”<sup>13</sup>.

By implementing a data-centric architecture, the U.S. Intelligence Community hopes that data will not be treated as a byproduct of the intelligence cycle, but as a key resource that drives decision-making and operational efficiency. One of the most important aspects of this transformation is reducing data security to the data object level, using technologies such as the Trusted Data Format<sup>14</sup> and the CCEB<sup>15</sup> - approved Zero Trust Data Format<sup>16</sup>. This allows the Intelligence Community to ensure data is secure and can be effectively shared across multiple platforms and accessed by global partners and allies. This exceptional level of security is essential to maintaining the integrity and confidentiality of classified information while facilitating intelligence interoperability. In the U.S., the Information Technology Roadmap provides a solid framework for modernizing the

---

<sup>13</sup> *Ibidem*.

<sup>14</sup> Trusted Data Format (TDF) is a specification for encoding data objects used to enable data tagging and the application of cryptographic security functions. These functions include confirming data properties or tags, cryptographic binding, and data encryption. TDF is available free of charge, without any restrictions, and does not require the use of proprietary or patented technology, making it accessible to anyone. TDF is the first interoperable data security solution connecting the Intelligence Community, the U.S. Department of Defense, and NATO member states.

<sup>15</sup> CCEB – NATO Combined Communications Electronics Board.

<sup>16</sup> Zero Trust Data Format (ZTDF) is a data-centric security approach that embeds encryption, access controls, and tamper-proofing directly into data objects, ensuring their self-defense and enabling secure sharing across security domains. It is designed to work in cloud, hybrid, and borderless environments, ensuring data is protected regardless of its location and access method.

U.S. Intelligence Community's IT infrastructure, enabling it to fully leverage its information assets, enabling more informed decision-making and more efficient operations – ultimately crucial for maintaining a strategic advantage in a data-driven world.

### **The Impact of New Technologies on Traditional Intelligence Collection Humint – Challenges for Long-Term Espionage Practice**

The awareness that digital technology has complicated human intelligence (Humint) officers' operational activities became apparent over 20 years ago. Just as the development of end-to-end encryption<sup>17</sup> has made conducting electronic intelligence (SIGINT) more difficult, the development of „ubiquitous technical surveillance” has made it more difficult for intelligence officers to conceal their identities, travel under pseudonyms, and meet with agents. The counterintelligence regime is stronger, more pervasive, and more hostile. For example, using new information and communication technologies as part of the „war on terror”, the US National Security Agency (NSA) collected telephone records in Pakistan, stored the collected data on cloud servers, and employed advanced statistical algorithms to identify individuals who made suspicious travel reservations. For example, someone who traveled more frequently than usual to tribal areas in the country, frequently changed phones or SIM cards, and frequently removed the battery from their phone became a suspect. In this way, NSA algorithms were able to identify al-Qaeda couriers „with a very low false positive rate, according to the agency”. Al-Qaeda leaders were eliminated en masse.

But using these typically intelligence-based methods of identifying individuals, counterintelligence services target individuals connected to intelligence services. In 2003, the CIA kidnapped Egyptian cleric Abu Omar from Milan. Italian police quickly identified the agents by tracking their phones. In 2010, a team from the Israeli intelligence agency Mossad assassinated a high-ranking Hamas member in Dubai. The members of the execution team followed all operational protocols. They came from various locations and were of different nationalities. However, within a month, officials from the United Arab Emirates collected camera footage, travel records, and call logs and unmasked the killers. „The experience of long-standing intelligence operational practices has been completely discredited”, Duyan Norman, former Deputy Director of the CIA's Technical Services Directorate, summarized the situation<sup>18</sup>.

<sup>17</sup> End-to-end encryption is a communication security method in which only the sender and recipient have the keys to decrypt the message. No third parties, including service providers, have access to the message content during transmission. This means that even if the message passes through intermediary servers, it cannot be read along the way.

<sup>18</sup> M. Devost, *Duyane Norman on Disrupting the CIA to Deal with Emerging Threats*, <[https://oodaloo.com/oodacasts/intelligence/duyane-norman-on-disrupting-the-cia-to-deal-with-emerg-](https://oodaloo.com/oodacasts/intelligence/duyane-norman-on-disrupting-the-cia-to-deal-with-emerg-223)

There are three main areas of intelligence activity in human intelligence (Humint), which are being significantly and negatively impacted by the development of modern technologies.

First, intelligence officers traveling under assumed aliases – essentially with false identity documents – can be exposed by biometric border controls, which identify discrepancies between physical characteristics and the names associated with them. Even if spies use a single alias for each country, they can still be tracked because friendly countries share biometric data. Operational algorithms that were feasible in the 1990s no longer work. Furthermore, any enterprising immigration officer can use Google Maps to instantly query an undercover intelligence officer for details about their personal life, such as their childhood commute to school, thus verifying their „legend”.

The second problem is that, operational activities, such as meetings with agents or the use of safe houses, stashes, or clandestine locations, are now subject to unprecedented counterintelligence scrutiny. Phone location data is widely available. Video surveillance has expanded to unprecedented levels. China alone has over 700 million surveillance cameras, many of which are equipped with facial recognition software or gait tracking. Russia, in turn, hopes to integrate all its cameras into a nationwide surveillance network.

Third, the disclosure of intelligence activity can be retroactive. For example, the killing of a Hamas official in Dubai was not monitored in real time. The killer was identified after the fact, after establishing his ties to the Mossad and presenting digital evidence that ruled out any Israeli denial. So-called „retroactive surveillance”, is not a new concept. Today’s so-called „digital dust” has physical roots. The Stasi, the East German intelligence service, preferred to mark so-called „targets” (those being tracked) with radioactive markers, using portable Geiger counters to track their movements. The Stasi also collected, stored, and catalogued target scents from fabrics removed from chairs the subject was sitting in. A Western intelligence officer could „lose sight” and, confident that no one was watching him, visit a dead-end alley with a stash of intelligence materials, unaware that interested parties could reconstruct his route.

Another problem is that in the age of the internet and social media, any contacts between individuals and intelligence agencies are very difficult to conceal. Addressing this issue, Michael Allen, former director of the U.S. House of Representatives Intelligence Committee, stated: „People tell me we might have to go back to the old days, when we were tapped on the shoulder in college and asked to join the CIA. We live in a time when our adversaries will be able to track anyone who ever used cia.gov”. What the intelligence community calls

---

ing-threats/#:~:text=Duyane%20Norman%20spent%20nearly%2030%20years%20in%20the,of%20the%20CIA%20Counterterrorism%20Center%E2%80%99s%20Incident%20Response%20Team> (29.04.2022).

„Ubiquitous Technical Supervision” (UTS) has made conducting human intelligence (Humint) in the field more difficult and expensive in many regions of the world. According to Dawn Meyerricks, who worked in the CIA’s technical division in 2018, „agent intelligence today is more of a technical business”. „The number of face-to-face meetings with agents is decreasing because such encounters carry enormous risks for both the intelligence officer and the agent”. According to her research, „in 30 countries, the technical level of counterintelligence regimes was so high that local security services did not need to track agency employees to know where they were”<sup>19</sup>.

However, despite the limitations outlined above, human intelligence remains crucial in ensuring national security. Electronic eavesdropping can reveal military plans, but only the agent can assess how seriously such plans should be taken. Furthermore, interpersonal communication is often nonverbal, relying on tacit knowledge that is not stored on computers, text messages, or in any other written form. Furthermore, human intelligence (Humint) and technical intelligence operations typically complement each other. The execution of the most complex, technical intelligence tasks most often depends on agents. America and Israel might never have launched the Stuxnet cyberattack on the Iranian nuclear facility in the 2000s if a Dutch engineer had not implanted malicious programming code into the Buser power plant’s control system via a USB drive. Despite this, operative activity is becoming increasingly difficult, costly, and risky. Human intelligence officials argue that there will always be loopholes in counterintelligence operations that allow for the recruitment and exploitation of agents. As new technologies advance, many old tenets of the trade are becoming relevant again. Generally, intelligence officials respond to UTS (Universal Technical Surveillance) in three ways:

First, rigorous adherence to operational techniques. „Most intelligence officers have always known that cover can’t be relied on”, says John Sipher, former CIA station chief in Moscow, adding that „spies will have to resort to old methods once used in countries like Russia and China”. Another option, says this veteran operations officer, is to conduct operations in places where surveillance is less intense: in cities where crowds can obscure cameras, in rural areas where surveillance is more limited, or in neutral countries<sup>20</sup>. This is one reason why cities like Helsinki and Vienna were swarming with spies during the Cold War. Yet another approach is to rely on intelligence officers, who are less likely to be the focus of counterintelligence attention. Intelligence agencies typically prefer to operate from embassies under diplomatic cover because it provides a certain

<sup>19</sup> *CIA agents tracked by technology in 30 countries*, <<https://nexusnewsfeed.com/article/geopolitics/cia-agents-tracked-by-technology-in-30-countries/>> (23.04.2018).

<sup>20</sup> *Stories of Spycraft: Former CIA Chief of Station John Sipher on Russia and Clandestine Services*, <<https://www.bing.com/videos/riverview/relatedvideo?q=John+Sipher%2c+a+-former+CIA+station+chief+in+Moscow>> (29.12.2021).

level of security. If you're caught spying, you'll be expelled, not imprisoned or shot. However, as technology makes it easier for counterintelligence agencies to track diplomatic personnel and distinguish intelligence officers under diplomatic cover from professional diplomats, intelligence agencies will be forced to rely more on those officers for whom a „natural” or, as the Americans call it, „unofficial” cover has been created.

Secondly, undercover intelligence. Personnel intelligence conducted under the guise of various export-related companies is nothing new. Long before the Cold War, intelligence agencies used newspapers, companies, and international organizations as fronts. Today's challenge is to create a cover identity for these companies that will withstand increased counterintelligence scrutiny. In the 2010s, the CIA banned the use of operationally created front companies. According to Zach Dorfman and Jenna McLaughlin<sup>21</sup>, two authors of studies on intelligence, the agency preferred to use real companies, often hiring their existing employees and training them separately in intelligence operations. The CIA also manipulated online data, such as websites about a given company's origin and activities, using access to government databases. Effectively ensuring full credibility of a company, known as legitimization, increasingly requires close cooperation with allies.

Third, new technologies in operational work. One way to minimize operational risk is to limit contact between officers and their agents. As early as the 1960s, Western intelligence agencies began using Short-Range Agent Communication (SRAC) devices, which allowed agents to send messages in short bursts near a specific location. These devices allowed for the transmission and reception of information from an agent located several dozen (hundreds) meters away, eliminating the need to „walk around the park with the agent”. SRAC is short-range, one-way or two-way wireless communication used for intelligence purposes. This communication technology was made possible by the advent of transistors and small-scale integrated circuits. SRAC devices were adopted by Western intelligence agencies during the Cold War in the 1960s, but Eastern Bloc countries possessed and utilized similar technologies. The devices are miniature for concealment and allow for the transmission of encrypted data. Examples of the American CDS-501 set were captured in Cuba and are believed to have been used in Central and Eastern Europe. The device operated in the upper VHF band and transmitted high-speed bursts of encrypted data from an agent to a receiving station located in a Western diplomatic mission in a hostile country to avoid interception by hostile electronic intelligence services. A high-ranking American intelligence source in Poland during the Cold War, Colonel Ryszard Kukliński, is believed to have used an SRAC device shortly before his defection to the West

---

<sup>21</sup> Z. Dorfman, J. McLaughlin, *The CIA's communications suffered a catastrophic compromise. It started in Iran*, Yahoo News, <<https://www.yahoo.com/news/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1>> (02.11.2018).

in late 1981. Another type of SRAC device was designated the RT-519 and operated in the VHF band. Former British intelligence officer Richard Tomlinson mentioned such SRAC devices, the size of a cigarette pack, in his book „The Big Breach: From Top Secret to Maximum Security”. The message text was first typed on a computer and then transmitted to the SRAC device. When the agent came within range of the receiving station, typically installed in British diplomatic missions, the device immediately transmitted the message<sup>22</sup>. In 2006, Russian authorities accused the UK of conducting espionage operations in Moscow and discovered a fake stone containing an electronic cache allegedly used by British agents in Russia. The device likely exchanged short data packets with PDAs owned by MI6’s Moscow station.

But these technologies don’t always work. Security flaws can lead to agents being exposed. In the 2000s, the CIA developed hundreds of secret communications websites (COVCOM), with hidden messaging functions, to enable communication with less valuable agents in countries like China, Iran, and Russia. These websites were not only poorly designed, revealing hidden code, but also poorly secured – IP addresses were logged sequentially, which, once one agent was exposed, allowed others to be exposed. Between 2009 and 2013, China and Iran hacked these systems, arresting and killing numerous agents. And yet, operational work, the discovery and acquisition of agents, and the management of an agency are based on trust. Intelligence officers want to look a potential agent in the eye, assessing their honesty, reliability, and personality. It’s not uncommon for agents to be eager and enthusiastic during their first meeting, inspired by the prospect of working with intelligence, but quickly become hesitant. In situations of uncertainty, they may confess to local authorities. A good approach is a „re-enlistment” two or three days after the initial meeting to strengthen the relationship. A few hastily sent text messages won’t accomplish this and won’t establish the case officer as a trustworthy, friendly mentor.

### **Global Intelligence is Moving to Cyberspace**

Digital technology has now permeated every corner of our lives. There are now 8.5 billion smartphones in the world, part of a microelectronics revolution that has dramatically reduced the cost of producing cameras, microphones, GPS receivers, and other sensors. As global internet penetration has increased from 35% in 2013 to 67% in 2023, these sensors—in phones, computers, cars, and televisions—have been connected, creating „intellectual factories” in every pocket, on every street. The algorithms and computing power required to understand this flood of data have also become exponentially more efficient and effective. This situation has also changed the priorities of intelligence. Intelligence agen-

---

<sup>22</sup> R. Tomlinson, *The Big Breach: From Top Secret to Maximum Security*, Global Pr 2001.

cies are tasked not only with tracking competitive technologies (e.g., is a rival secretly developing a new artificial intelligence model?) but also with determining how it will be used. In the United States, for example, intelligence agencies are weighing in on the public debate over whether they are concerned about Chinese influence on internet-connected products, from TikTok to routers and autonomous cars, and whether these products could become tools for data collection, political interference, or sabotage in wartime.

### **Signals Intelligence (SIGINT) is evolving into intelligence activity in cyberspace**

Twelve years ago, Edward Snowden, a disgruntled employee of the National Security Agency (NSA), the US signals intelligence agency, fled to Hong Kong and then to Russia and revealed that America and its allies were intercepting a significant portion of global communications. US intelligence agencies warned at the time that his revelations would have dire consequences, as enemies found alternative means of communication. Ultimately, the situation was not as dire for the United States and its allies as feared. Intelligence agencies hostile to the US did not gain access to „all the data they needed, some of which they had previously had access to”, writes Ciaran Martin<sup>23</sup>, then a senior official at the British signals intelligence agency GCHQ. „However, they could have obtained much”, he notes. Over recent decades, as information transmission technology has advanced, the nature of signals intelligence (SIGINT) has changed. In the 1990s, the internet replaced radio and telephone. Now, more than a decade after Snowden, a significant portion of internet traffic is encrypted, and data is stored in new places, such as the cloud. Computer networks have become an integral part of the physical world, from cars to power grids to military systems. The lines between cyberespionage and cyberattacks are blurring, somewhat changing the identity of intelligence agencies. The development of encryption has certainly made life more difficult for police. In 2022, 92% of encrypted data intercepted by US federal agencies could not be deciphered. This is not a particular problem for data transmitted by domestic US institutions and companies. In legally sanctioned cases, agencies simply request declassification and handover of the necessary data. US laws, including the Cloud Act of 2018 and Section 702 of the Foreign Intelligence Surveillance Act (FISA), renewed and expanded in April 2024, require companies to hand over a wide range of data, even if it is stored abroad.

But intelligence isn't always dependent on the specific content of transmitted and intercepted transmissions. Information about who is sending encrypted data

---

<sup>23</sup> Ciaran Martin served as a senior civil servant at GCHQ, where he played a key role in establishing the National Cyber Security Centre (NCSC) and strengthening the UK's cybersecurity efforts.

and so-called metadata<sup>24</sup> to whom is invaluable. This „traffic analysis” was crucial to Western policy during the Cold War and in the post-9/11 era. It remains relevant today. “If you have enough metadata, you don’t need the content” - notes Stuart Baker, a former NSA lawyer<sup>25</sup>. This explains why collection of raw internet traffic remains useful. In March 2024, justifying new, more stringent intelligence regulations, the Dutch government explained that „hosting the world’s largest internet communication hubs obliges us... to make optimal use of the data flowing through our cables to protect the Netherlands from Russian and Chinese hackers”. An alternative approach is to deliberately weaken encryption so that it can be broken with less computational effort. Matt Blaze, a cryptography expert at Georgetown University, is skeptical about the effectiveness of such measures. He claims that „the world of civilian cryptography has reached a level where people can recognize deliberate weaknesses quite well”<sup>26</sup>. Another approach involves extracting data from a phone or computer - or, in cyber specialists’ jargon, from the so-called „endpoint”. Snowden revealed that the NSA had devoted enormous resources to cracking them. Since then, the sums spent on this type of cyber intelligence have only increased. So called, zero-day effects<sup>27</sup> are snippets of code that target previously undetected software vulnerabilities. They are rare, expensive, but very useful in gaining access to specific devices. Worse still, the barriers to entry for this type of code have virtually disappeared, fostering the emergence of a cottage industry of espionage. It is estimated that over 40 percent of zero-day effects are used in commercial spyware, which not only hacks phones but also transforms their microphones and cameras into hidden sensors. The most prominent example of such software is Pegasus, created by NSO Group, an Israeli company dominated by veterans of Israeli intelligence. According to reliable reports, Pegasus has been used repeatedly in hacking operations against dissidents, journalists, and activists worldwide. In February 2024, the US government, which had previously blacklisted NSO Group and three other companies, also announced visa restrictions for individuals involved in the abuse of this spyware.

---

<sup>24</sup> Metadata is data about data. It describes other data, facilitating its organization, retrieval, and management. It can include, for example, the structures of tables in databases, fields in files, or document characteristics. It is crucial for the effective use and reuse of data. Metadata analysis can, among other things, reveal details about user activity, such as phone calls, location, or network activity.

<sup>25</sup> D. Cole, *We Kill People Based on Metadata*, <<https://www.nybooks.com/online/2014/05/10/we-kill-people-based-metadata/>> (10.05.2014).

<sup>26</sup> *Signals intelligence has become a cyber-activity*, <<https://www.economist.com/technology-quarterly/2024/07/01/signals-intelligence-has-become-a-cyber-activity>> (01.07.2024).

<sup>27</sup> The effects of zero-day attacks can be severe and include data theft, system compromise, service disruption, financial loss, reputational damage, and the disruption of critical infrastructure. These attacks exploit software vulnerabilities that vendors are unaware of or haven’t yet patched, giving attackers an advantage.

Intelligence agencies are increasingly using ransomware<sup>28</sup>. Observing the development of cyber intelligence, it's worth noting the methods used by cyber spies (cyber espionage agents) working for state intelligence agencies. Currently, the line between cyberespionage and cyberattacks on IT networks is blurring, creating certain operational dilemmas. If you disrupt a network, you're likely to be caught and eliminated by the network owner. Meanwhile, data theft or clandestine modification is rarely disclosed. According to a report published by SentinelLabs<sup>29</sup>, cyber intelligence groups linked to China are increasingly using ransomware as a phase of intelligence operations, aimed at distracting adversaries from their operations while also hindering the publication of inconvenient information and generating revenue. Historically, cyber intelligence groups operating on behalf of nation states have avoided the use of ransomware, a typical cybercriminal tactic, but this situation appears to be changing. State-backed hackers are increasingly using ransomware to conceal their activities. State-sponsored cyber intelligence disguised as ransomware creates „opportunities for hostile states to legitimize their activities by attributing them to independent cybercriminals rather than state-sponsored organizations”, Alexander Milenkoski, senior threat researcher at SentinelLabs, and Julian-Ferdinand Voegele, threat expert at Recorded Future, wrote in a report<sup>30</sup>. According to these experts, „mislabeling cyberespionage as a purely financial cybercrime can have strategic implications, especially when suspected ransomware attacks target governments or critical infrastructure institutions”. Attempts to restore systems after a ransomware attack and recover as much encrypted data as possible also work to the advantage of cyberespionage groups, who can impersonate specialists trying to remove the effects of a ransomware attack and carry out attacks that destroy objects associated with the intrusion, while making it difficult to identify the potential culprits.

Senior US officials are sounding the alarm about what they believe is China's aggressive cyberthreat to sensitive US civilian networks, typically without obvious espionage value. According to these officials, a prime example of this type of activity is the activity of cybercriminals from a group commonly referred to as „Typhoon Volt”<sup>31</sup>, which aims to influence US decision-making in the

---

<sup>28</sup> Ransomware – a type of malware that blocks access to a computer system or encrypts data, and then demands a ransom to restore access or decrypt files.

<sup>29</sup> *12 Months of Fighting Cybercrime & Defending Enterprises | SentinelLABS 2024 Review*, <<https://www.sentinelone.com/blog/12-months-of-fighting-cybercrime-defending-enterprises-sentinelabs-2024-review/>> (02.01.2025).

<sup>30</sup> A. Milenkoski, J-F Voegele, *ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware*, <<https://www.sentinelone.com/labs/chamel-gang-attacking-critical-infrastructure-with-ransomware/>> (26.06.2024).

<sup>31</sup> Volt Typhoon (also known as VANGUARD PANDA, BRONZE SILHOUETTE, Redfly, Insidious Taurus, Dev-0391, Storm-0391, UNC3236, or VOLTZITE) is a highly sophisticated group of cyber experts purportedly providing cyber intelligence for the People's Republic

event of a conflict. The use of ransomware in China-related cyber operations is not without precedent. Researchers from Mandiant have previously detailed the activity of the APT41 group, which includes state-sponsored espionage activities as well as „financially motivated activities that potentially fall outside the control of the state”. According to a July 2023 Mandiant analysis<sup>32</sup>, ransomware in state-led operations temporarily distorts attribution and amplifies the psychological aspect of a specific operation. Ransomware can also be useful as a smokescreen, used to identify a potential adversary. „It’s partly about intelligence gathering, and also about understanding what they could do if they really wanted to attack with much more malware. This kind of activity almost feels like a war game”. In turn, a June 25, 2024, study<sup>33</sup> identified a distinct type of cyber activity, using off-the-shelf tools, targeting American manufacturers across various industries in North and South America and Europe. The purpose of these activities is less clear, but the method employed bears some resemblance to previous activities by hacking groups from China and North Korea.

## **New technologies promote the commercialization of intelligence**

### **Private companies are creating new opportunities for intelligence agencies to acquire data in cyberspace**

The influx of massive amounts of data, primarily from the internet, is fueling a boom not only in state intelligence but also in the private intelligence sector. This sector often strengthens the operations of intelligence agencies by providing them with new tools and expanding access to unclassified data that can be shared with the public and allies. To some extent, the private sector also relieves these agencies of the burden. For example, private cybersecurity companies are as important in this sector as Western intelligence agencies. However, the boom in the

of China. The group, active since at least mid-2021, is known for attacks on critical infrastructure in the United States. Volt Typhoon focuses on espionage, data theft, and credential access. According to Microsoft, its campaigns prioritize identifying opportunities to sabotage critical communications infrastructure between the United States and Asia in potential future crises. The U.S. government believes the group’s primary goal is to slow a potential U.S. military mobilization that could follow a Chinese invasion of Taiwan. Volt Typhoon is believed to be commanded by the People’s Liberation Army Cyber Forces. The Chinese government denies the existence of this group.

<sup>32</sup> *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*, <<https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools>> (03.06.2024).

<sup>33</sup> *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, <<https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion>> (10.07.2024).

private cyberintelligence services market also poses a significant challenge for intelligence agencies, as the boundaries between what is public and what state intelligence services can do and what others can do are blurring. With the growth of data, its disclosure, and its significance for geopolitical rivalry, questions about law, ethics, and privacy arise. „The separation of private and public interests is a uniquely Western construct”, argues Duyane Norman, a former CIA officer. „It brings enormous benefits, but it can also have serious consequences”<sup>34</sup>. At the heart of this revolution is the internet. Christopher Ahlberg, who heads Recorded Future<sup>35</sup>, a company that tracks cybercriminals online, argues that „traditional espionage is ‚dead’ because of technology”. He believes modern intelligence should move to cyberspace. „We couldn’t build our businesses without the internet as our primary source of data. Yet, everything ends up online these days”, he says. The anonymity of the deep web, which isn’t indexed by search engines, and the dark web, which requires specialized software to access, make them perfect locations for terrorists, pedophiles, and criminals. However, this anonymity is often superficial. Flashpoint<sup>36</sup>, a well-known platform for recognizing and combating cyber threats, began by using fake identities. This company’s analysts impersonated potential jihadists, infiltrating extremist groups online and gaining information about their intentions. The company continues to do this, but its primary focus is now data. For example, it tracks „wallets” where extremist groups store Bitcoin and other cryptocurrencies. The flow of funds into and out of such „wallets” can indicate an impending terrorist attack.

PrimerAI<sup>37</sup>, a company with similar expertise, used cyber intelligence to warn the US government of a cyber threat eight hours in advance, identifying hackers boasting of preparations for an attack on the deep web. In this case, the company used natural language processing, a form of artificial intelligence, to analyze large amounts of text, including confidential customer data.

Some private cyber intelligence agencies operate using a different model. Instead of observing threats evolving online, they track them from the network level. Companies that create critical IT hardware or software possess unparalleled

---

<sup>34</sup> NBC News: *Former CIA officer says traditional spying is ‚dead’ due to technology, internet*, <<https://www.yahoo.com/news/former-cia-officer-says-traditional143030382.html>> (07.10.2021).

<sup>35</sup> Recorded Future, a digital platform that provides comprehensive, objective, real-time threat intelligence by combining internal and external telemetry data using AI-powered Intelligence Graph® software. The Intelligence Graph indexes, organizes, and analyzes data from over a million sources, including the open web, dark web, technical channels, and customer telemetry.

<sup>36</sup> Flashpoint is an industry leader in threat intelligence and analytics. It combines human-driven data collection and analysis with intuitive technology to help clients make fast and decisive decisions to stop threats and mitigate risk.

<sup>37</sup> PrimerAI Technologies, Inc., based in San Francisco, specializes in helping organizations maximize their data investments by applying cutting-edge machine learning and natural language processing technologies.

knowledge of private traffic flowing through their networks. For example, Google dominates email, Microsoft dominates operating systems, and Amazon dominates cloud computing. As a result, these corporations possess extensive private signals intelligence (SIGINT) capabilities, information from which can be sold to clients as a security service. „Microsoft monitors 78 trillion ‚signals‘ per day (such as connections between a phone and a cloud server)”, says Sherrod DeGrippe, director of threat intelligence strategy at the company<sup>38</sup>. Analysts look for anomalies in this data and monitor the tools, infrastructure, and activities of state-backed or criminal hacking groups, known as advanced persistent threats (APTs). In certain circumstances, the law allows Western intelligence agencies to „break” the laws of the countries in which they operate, for example, by bribing foreign officials. Private companies cannot do this; they operate under the rules of commercial intelligence. However, they have other advantages. Ahlberg, the previously mentioned representative of Recorded Future, states, among other things, that by conducting intelligence operations in cyberspace, companies „can combine their infrastructure and capabilities to launch an attack in a way that intelligence agencies cannot”. He points out that „intelligence agencies have the right to operate freely abroad, but not domestically”. Meanwhile, private corporate intelligence agencies „can operate not only abroad but also, in a unique way, conduct reconnaissance within a country”. It is also worth noting the intermingling of personnel between state and commercial intelligence agencies. Intelligence analysts often travel between intelligence agencies and threat analysis companies, sharing their knowledge. Lewis Sage-Passant, head of intelligence at a large pharmaceutical company in Europe, argues that „internal intelligence teams within companies are fierce competitors to intelligence groups in other companies, but technically they remain allies and speak with each other almost daily”<sup>39</sup>.

Many companies jealously guard their data and maintain secrecy about their methods and clients. But sometimes, these same companies can be surprisingly open to foreign competitors. In practice, private companies often monitor the same hacker groups from China, Russia, North Korea, and Iran as intelligence agencies.

### **Commercialization of Imagery Intelligence – IMINT**

The growth of the commercial satellite industry allows the intelligence community to almost fully meet its IMINT needs. For example, the UK intelligence community previously leveraged the capabilities of commercial companies by purchasing commercial satellite imagery. „Back then, these purchases cost the British government

<sup>38</sup> *Private firms and open sources are giving spies a run for their money*, The Economist Report: Watching the watchers, <<https://www.economist.com/technology-quarterly/2024/07/01/private-firms-and-open-sources-are-giving-spies-a-run-for-their-money>> (01.07.2024).

<sup>39</sup> *Ibidem*.

hundreds of thousands of dollars annually. However, today, the scale of these purchases is many times greater, reaching many millions of dollars”, says British General Sir Jim Hockenhull<sup>40</sup>. The commercialization of IMINT, and satellite intelligence in particular, also allows for closer cooperation among allies. In the past, there were situations where a country’s intelligence service had information on a specific matter but could not share it with allies for fear of disclosing the source. According to Aaron Bateman of George Washington University, „this phenomenon was common in space intelligence. During the Cold War, America rarely shared satellite imagery, even with its NATO allies”<sup>41</sup>. Today, commercial satellite imagery is regularly published. According to Bateman, state intelligence agencies also outsource satellite reconnaissance and intelligence gathering tasks to external analysts. As a result, state intelligence agencies have an additional „manpower that the US government doesn’t have to pay for, and which still brings tangible benefits”<sup>42</sup>.

Joe Morrison of UMBRA, a startup specializing in radar satellites, recalls being asked by Western officials why they were forced to work with commercial, transparent suppliers. „I told them: Because of access to talent who like to smoke pot”<sup>43</sup>. He wasn’t kidding. Intelligence agencies offer young, talented people the opportunity to work in organizations with a rich history and a patriotic mission. However, the year-long wait for security clearance, low salaries compared to private companies, and the lack of remote work options can pose significant barriers for many of them. This situation means intelligence agencies are currently facing significant challenges related to reorganizing the methods and processes of gathering information. This problem was recognized and presented in a paper published by the Alan Turing Institute in November 2023 by Lucy Mason, a former British defense official, and Jason M., an active British intelligence officer. „The British intelligence community... faces an existential challenge”, they argued. „We need to move away from a model in which national security is handled by a few individuals in highly centralized, secret organizations”. Indeed, this activity is already „being displaced by open-source information and intelligence providers”. A solution to these current problems would be a new intelligence model that „accepts that data, obtained from mobile apps and sold by advertising intermediaries, would be routinely used by intelligence agencies”<sup>44</sup>.

---

<sup>40</sup> *Artificial intelligence can speed-sort satellite photos*, “The Economist”, <<https://www.economist.com/interactive/international/2023/01/13/open-source-intelligence-is-piercing-the-fog-of-war-in-ukraine>> (23.06.2023).

<sup>41</sup> A. Bateman, *Mutually assured surveillance at risk: Anti-satellite weapons and cold war arms control*, “Journal of Strategic Studies” 2022, Vol. 45, Issue 1, pp. 119-142, published online: 26.01.2022.

<sup>42</sup> *Ibidem*.

<sup>43</sup> *Ibidem*.

<sup>44</sup> L. Mason, Jason M., *Emerging from the Shadows. Redesigning the UK’s security apparatus for a more prosperous future*, CETaS Expert Analysis 28 November 2023.

## OSINT in the Digital Revolution<sup>45</sup>

OSINT (from Open Source INTelligence), which can be translated as „open source intelligence” or open-source intelligence, is the activity of obtaining information from open and publicly available sources. The basis for all data recording, sharing, and retrieval, regardless of its type – from computer code to grandfathered war stories and public accounting records – is language. OSINT activities are no different. OSINT practitioners collect and evaluate human-generated content using open-source language (natural language), as well as using human language encoded using computer languages into a form understandable by computers, using queries formatted to a specific computer language structure. The explosion of information technology has made life with OSINT both easier and more challenging. Easier due to the widespread access to information across numerous telecommunications channels, and more difficult due to the equally widespread dissemination of junk or misleading information. Effective verification of the content of obtained data has become a serious problem. This means that OSINT must not only collect and process digital data but also develop mechanisms for its verification and attribution<sup>46</sup>, as well as understand what constitutes junk content and what does not. To assess which digital information or types of data are important from an intelligence perspective, intelligence services require technical infrastructure and high-quality specialists (or appropriate outsourcing<sup>47</sup>) to understand the internet and its constantly changing patterns of data distribution and storage. To this end, most intelligence agencies using OSINT have begun to create separate structures dedicated to internet research<sup>48</sup>. Furthermore, intelligence agencies, which have always competed with each other in obtaining information, now must not only compete with each other but, due to the widespread public availability of online sources, also compete with individual analysts and analysts from private companies using OSINT tools. From counterterrorism to cybersecurity, from monitoring weapons of mass destruction to analyzing protests – in the case of OSINT, technology companies and so-called „civilians” utilize the same types of data and information as most state intelligence services. While non-state analysts lack the financial

---

<sup>45</sup> K. Surdyk, *OSINT w epoce Wielkich Zbiorów Danych (Big Data)*, „Przedsiębiorstwo Przyszłości” 2022, No 3 (52), pp. 33-56.

<sup>46</sup> Attribution – the attribution of certain characteristics to someone or something. In psychology, the concept of attribution refers to how people explain the causes of their own or others’ behavior, so-called naive theories of causality. This term also appears in Polish grammar and exists in the field of business marketing.

<sup>47</sup> Outsourcing (short for outside-resource-using) – separating some of the functions performed independently from the organizational structure of an enterprise and transferring them to other entities for execution.

<sup>48</sup> E.J. Appel, *Cybervetting. Internet Searches for Vetting, Investigations, and Open-Source Intelligence*, Second Edition, CRC Press 2014, p. 157.

resources of state intelligence agencies, they more than compensate for this lack with autonomous and rapid operations, as well as the ability to improvise. In addition to the above, one of the new aspects that must be considered in modern OSINT is the issue of so-called „Big Data.” The „Big Data” revolution has brought with it often-predicted innovations such as new data storage and transmission technologies, the availability of 3G/4G and 5G data networks, as well as mass access to Wi-Fi and cloud technologies, thanks to which we are now able to create, store, and share unprecedented amounts of information. These technologies make the production, storage, or transmission of a single unit of data (a byte) increasingly affordable. It also enables the generation and collection of social data (especially personal data) with a high degree of detail. Ultimately, our personal data, data on our activities, behaviors, opinions, etc., serve not only the administrative or statistical purposes for which they were created, but also advertising and even criminal purposes. For example, our tax or employment data can be used to profile our purchasing behavior, healthcare options, residential choices, voting behavior, and so on. News, blogs, social networking data, music, films, books, and scientific articles are all taking digital form. Vast collections of books, including the most renowned libraries, are being digitized. Searching these collections using modern OSINT tools is possible using keywords, provided, however, that the lack of thematic hierarchy, the inability to focus on a specific topic, and the inability to analyze links between documents are taken into account<sup>49</sup>. Although OSINT tools are evolving rapidly, the most popular methods for obtaining intelligence from publicly available digital collections can be divided into four main categories:

- linguistic/textual methods,
- methods using geographic information systems (GIS) – remote sensing,
- methods based on network theory,
- methods using visual forensics.

A detailed discussion of these methods is beyond the scope of this article, but it's worth briefly outlining the results that can be achieved by using them.

And so, while text-based OSINT can be implemented using standard programming, dedicated text-based OSINT applications also exist. Some allow users to detect and visualize connections, patterns, and themes in large amounts of text. Furthermore, natural language processing applications based on statistical topic modeling, such as Latent Semantic Analysis/Indexing (LSA/I)<sup>50</sup> or Latent Di-

---

<sup>49</sup> D. Brzeziński, *Top modeling*, Politechnika Poznańska Instytut Informatyki, <[https://www.cs.put.poznan.pl/alabijak/emd/11\\_Topic\\_modeling.pdf](https://www.cs.put.poznan.pl/alabijak/emd/11_Topic_modeling.pdf)> (21.12.2016).

<sup>50</sup> Latent Semantic Indexing (LSI) or Latent Semantic Analysis (LSA) is a machine learning-based text analysis method that learns from sample text to identify „hidden” concepts in multiple documents.

richlet Allocation (LDA)<sup>51</sup>, facilitate cataloging, sorting, and processing large amounts of text data from social media, enabling OSINT analysts to detect behavioral patterns and analyze sentiment based on machine learning for retrospective or real-time analysis.

Furthermore, the combination of geographic information systems – GIS – and internet-based location data<sup>52</sup> (reports, location tags) allows analysts to exploit the broader social and spatial dynamics of human behavior, including mobilization, mass social movements, and conflicts.

One of the most popular applications of network analysis in digital OSINT is social media analysis, which involves tracking activity and likes on these media and sharing relationships among very large groups of social media participants. Compared to older methods, network analysis of social media enables more effective exposure of the hierarchy of a given social group and the influencers<sup>53</sup> operating within it.

However, thanks to methods based on image forensics, visual media can now be digitally analyzed, interpreted, and utilized to extract key information, for example, from areas affected by conflict, protests, or disasters where physical access is limited. Images and videos can be used for verification purposes, statements, propaganda, and counterpropaganda on the battlefield or during crisis episodes. They can also be shared as evidence of existing relationships, interests, and opportunities.

### **Old technologies are no worse than new ones in the operational and technical support of intelligence**

Robert Gates, director of the CIA from 1991 to 1993, once observed that every intelligence officer in the field needed a support person at headquarters<sup>54</sup>. This ratio has certainly increased today. This is primarily due to the increasin-

<sup>51</sup> Latent Dirichlet Allocation (LDA) is a text-based machine learning method similar to LSI, although LDA organizes words into a topic model independently rather than into user-defined folders. LDA examines the frequency and relationships between words in text based on how often they are used together and in what context.

<sup>52</sup> GIS – Geographic Information System – an information system used to enter, collect, process, and visualize geographic data, one of whose functions is to support the decision-making process. Every GIS system consists of a geographic database, computer hardware, software, and GIS developers and users.

<sup>53</sup> Influencer (from English: influence) – in the world of social media, an influential person who, thanks to their reach, is able to influence people, with whom they establish lasting relationships. They publish product reviews or informative articles in exchange for the opportunity to try a product or a financial bonus from a partner.

<sup>54</sup> T.J. Naftali, T.E. Masoud, *Transcript. Interview with Robert M. Gates. George H.W. Bush Oral History Project*, College Station, Texas, <<https://millercenter.org/the-presidency/presidential-oral-histories/robert-m-gates-deputy-director-central>> (23-24.07.2000).

gly refined counterintelligence operations, which are widely implementing new identification and surveillance technologies. Securing operational intelligence activities requires increasing personnel and technical resources, in areas such as legalization, intelligence electronics, intelligence mechanics and chemistry, as well as intelligence communications with their inherent encryption. However, it turns out that in some situations, technological advances in one field can lead to a return to traditional methods in another. A prime example is radio intelligence communications, which are coming back into favor as the age of quantum computers inevitably approaches.

### **Intelligence Communications**

Quantum technology dangerous to intelligence communications? Cryptography is an important element in securing intelligence communications. Encrypted messages safely reach their recipients without the risk of their content falling into the wrong hands. However, quantum computers are emerging on the horizon. These computers will likely be able to decrypt a significant portion of data encrypted using current encryption methods. Western experts fear that China is already collecting data to decrypt it when technology allows. At the same time, cryptographers are already working on algorithms resistant to quantum attacks. For example, Apple introduced such an algorithm for iMessage in February 2024, but it has not been implemented on a large scale. Counterintelligence agencies are obviously not keen on implementing such algorithms, as they are investing significant resources in building quantum computers. However, there are reasons to believe that quantum computers powerful enough for effective decryption will not be available until the 2030s.

Sometimes, old methods of intelligence communications are the best. Encrypted radio messages, long used in intelligence communications, are still alive and well. From the mid-1960s until 2008, anyone tuning their radio to the shortwave frequency between 5.422 and 16.084 MHz periodically heard the cheerful sound of a flute playing a few bars of an English folk song. Then a woman's voice with an English accent would read out the numbers: „Zero, two, five, eight...” These were believed to be encrypted messages from MI6. The „Lincolnshire Poacher”, named for its cheerful melody, was one of many „numbers stations” used by intelligence agencies to communicate with agents in the field. Some were dismantled at the end of the Cold War. However, many still transmit. Priyom.org, a website that monitors these stations, notes that their activity has “increased significantly” since the mid-2010s, with broadcasts using voice, Morse code and digital signals.

The question arises: why use radio transmissions when there are so many new data transmission technologies? An article by Tony Ingesson and Magnus Andersson from Lund University suggests that one reason is the lack of security in current

communication methods<sup>55</sup>. Providers of encrypted phones or applications have been hacked or manipulated by security authorities numerous times. Spyware is increasingly being used to infect phones. The authors conclude that it's safest to assume that „every device connected to the internet is at risk” for intelligence purposes. However, at least theoretically, radio numbers stations are unhackable. The sender and recipient use one-time pads<sup>56</sup> containing a list of random numbers, the same for encrypting and decrypting messages. Text encrypted using one-time pads (if used correctly) is undecipherable, even with a quantum computer.

Another problem remains. Radio surveillance services, based on intercepted transmissions (radio traffic analysis), can determine how many agents are active or at what time they are active on the air. To prevent identification of a specific agent's transmission, transmitters send fictitious „filler” transmissions, even when no message is needed. In 2007, cryptography expert Matt Blaze noticed that messages sent by the Cuban residency did not contain the number „nine”. His theory was that the random number generator used to generate the fictitious traffic was faulty<sup>57</sup>. Then, in 2020, FBI agent Peter Strzok published a book in which, without going into detail, he noted that, based on radio traffic analysis, the FBI was able to determine when messages were and were not sent to Russian „illegal” (deeply classified) intelligence agents in Massachusetts<sup>58</sup>. The conclusions that can be drawn from the above include the following:

- Firstly, old technology is often timeless, even in the age of the internet, and radio is more resistant to disclosure than computer software.
- Secondly, nothing can replace true intelligence craftsmanship.

### **Is Agent-Based Artificial Intelligence Possible?**

Most experts are positive about the future of AI in intelligence, although with some reservations. According to Admiral Whitworth<sup>59</sup>, „visual converters” – a subset of

---

<sup>55</sup> T. Ingesson, M. Andersson, *Clandestine Communications in Cyber-Denied Environments: Numbers stations and radio in the 21st century*, “Journal of Policing, Intelligence and Counter Terrorism” 2023, Vol. 19, No 2, pp. 144-165.

<sup>56</sup> One-time pad ciphers are an old encryption technology, widely used since before World War II. They are the only encryption technique whose security can be mathematically proven. Spies around the world have been using one-time pads (OTPs) since the 1940s. The reason for OTP's popularity among intelligence agencies is its transmission security. All intelligence transmissions from numbers stations are encrypted using OTP.

<sup>57</sup> *Matt Blaze on OTP Radio Stations*, <<https://www.schneier.com/blog/archives/2020/09/matt-blaze-on-otp-radio-stations.html>> (18.09.2020).

<sup>58</sup> P. Strzok, *Compromised: Counterintelligence and the Threat of Donald J. Trump*, Houghton Mifflin Harcourt 2020.

<sup>59</sup> Vice Admiral Frank Whitworth is the eighth director of the U.S. National Geospatial-Intel-

the „generative, pre-trained converters” that make up GPT60 in ChatGPT – hold great promise in intelligence. They could enable an AI model to provide context in natural language. For example, they could present not only an image of an identified missile battery but also a description explaining its deployment. British intelligence, in turn, is experimenting with tools that can generate automated combat orders based on the identified enemy force distribution. Skeptics, however, point to the human factor, which AI cannot replace. The same Admiral Whitworth notes that there is a significant difference between computer vision used in civilian intelligence and that used in military intelligence<sup>61</sup>. For example, in video surveillance related to facial recognition used in civilian intelligence, the face constitutes 80% of the field of view, and AI algorithms perform very well. A different situation occurs in military intelligence. A missile launcher, located in a forest and depicted in the corner of a satellite image, represents only two hundredths of a percent of that field. In this case, according to Admiral Whitworth, „the effectiveness of current AI algorithms is not high and can only be compared to that of a novice analyst”.

Despite some doubts, artificial intelligence is entering the world of intelligence. American intelligence officers already have access to tools like ChatGPT on their mobile phones, processing classified data. In May 2024, Microsoft announced that it had developed an „airborne” version of GPT-4, disconnected from the internet, for American intelligence agencies. However, some experts remain skeptical. In a paper published in 2023, researchers from the Alan Turing Institute think tank warned that AI cannot be trusted to produce pre-packaged intelligence reports, which require lateral thinking<sup>62</sup> and counterfactual reasoning<sup>63</sup>. They argued that this would require new hybrid models based on neural symbolic networks, which combine the statistical approach used in neural networks with old-fashioned, logic-based AI („if this, then that”). Those working with state-of-the-art models dispute this, arguing that intelligence agencies are too conservative<sup>64</sup>.

---

Intelligence Agency (NGA). He became director of the NGA on June 3, 2022.

<sup>60</sup> GPT (Generative Pre-Trained Transformer) – a type of large language model, or machine learning model, trained on large datasets and capable of generating text based on context. GPT is one of the largest and most advanced language models.

<sup>61</sup> *Artificial intelligence can speed-sort satellite photos. Could it also recruit an agent?*, <<https://www.google.com/search?client=firefox-b-d&q=Artificial+intelligence+can+speed-sort+satellite+photos>> (01.07.2024).

<sup>62</sup> Lateral thinking, also known as „outside the box” thinking, is a creative problem-solving process that involves finding new, unconventional solutions, often by departing from established thought patterns. The term was coined by Edward de Bono.

<sup>63</sup> Counterfactual reasoning, also known as counterfactual thinking, is the process of considering alternative scenarios that could have happened but did not. It involves imagining what would have happened if certain facts had been different.

<sup>64</sup> A. Janjeva, A. Harris, S. Mercer et al., *The Rapid Rise of Generative AI. Assessing risks to safety and security*, Research Report Centre for Emerging Technology and Security (CETaS), The Alan Turing Institute 16 December 2023, pp. 67-68, <<https://cetas.turing.ac.uk/publica-240>>

A recent study by Philipp Schonegger of the London School of Economics and his colleagues found that volunteers with access to LLM<sup>65</sup> made predictions that were 23% more accurate than a control group<sup>66</sup>. Others have gone even further in their assessments. Mark Warner, Chairman of the U.S. Senate Select Committee on Intelligence, stated during Senate hearings in September 2023, among other things: „A year ago, there was talk of a single, large language model that would encompass images, intercepted information, and files obtained by human intelligence (Humint)”<sup>67</sup>.

In practice, collecting large amounts of intelligence requires massive storage capacities, and running machine learning models requires enormous computing power. Therefore, some agencies have turned to cloud solutions to store classified data, creating secret cloud servers. However, according to Warner, „the idea of creating a common, sovereign AI technology for the entire Intelligence Community is not the right solution”. And this is not just about the limitations associated with processing vast amounts of data. If a secret cloud were to be used, lumping the data into a single bin would be problematic for intelligence security purposes. According to him, „the NSA will have its model, and the CIA can have its own”<sup>68</sup>.

To summarize the challenges of implementing AI systems in intelligence, it’s a process that requires overcoming a number of barriers, not just technical ones. This situation is well reflected in the words of Jason Matheny, who oversaw technology and national security policy at the White House until 2022, who stated that: “there’s a lot of critical work that needs to be done to prepare intelligence agencies for AI. There are bureaucratic and technical hurdles. It’s not just about building systems that can run modern software, but also about ensuring that databases within and across agencies are interoperable”<sup>69</sup>.

---

tions/rapid-rise-generative-ai> (28.12.2023).

<sup>65</sup> LLM (Large Language Model) - A language model trained on large amounts of data that enables text generation and natural language processing tasks. LLM models are trained using self-supervised or weakly supervised machine learning approaches using large amounts of text data.

<sup>66</sup> P. Schoenegger, P.S. Park, E. Karger et al., *AI-Augmented Predictions: LLM Assistants Improve Human Forecasting Accuracy*, <<https://arxiv.org/abs/2402.07862>> (12.02.2024).

<sup>67</sup> J. Hendrix, *Transcript: Senate Hearing Addressing the National Security Implications of AI*, <<https://www.techpolicy.press/transcript-senate-hearing-addressing-the-national-security-implications-of-ai>> (21.09.2023).

<sup>68</sup> *Ibidem*.

<sup>69</sup> *Artificial intelligence can speed-sort satellite photos*, “The Economist”, <<https://www.economist.com/technology-quarterly/2024/07/01/artificial-intelligence-can-speed-sort-satellite-photos>> (01.07.2024).

## Conclusion

To put it simply, intelligence is changing as the locations where information can be found change. The digital revolution has led to a dramatic increase in the importance of OSINT, a type of intelligence activity that utilizes open-source data, but in this case, leverages new data collection and analysis technologies, including those working with digital sources. While digitizing paper documents can help government agencies increase efficiency, improve communication, and streamline public services, most data will still remain unstructured. This is where Natural Language Processing (NLP) comes in, presenting a challenge for AI. Thanks to recent technological advances, computers can now read, understand, and use human language. They can even measure sentiment by tracking specific texts or the tone of speech, and enable government agencies to recognize patterns of social behavior, categorize important topics, and analyze public opinion.

In 2023, Richard Moore, head of the British intelligence agency MI6, announced that artificial intelligence was already helping intelligence work. “My teams are already using AI to supplement their own assessment of how humans might behave in different situations”, and in the future... as AI begins to take over some aspects of human cognition, digital tools will be better able to understand or predict human behavior than humans”<sup>70</sup>. In a working paper published in March 2024, researchers from the Swiss Federal Institute of Technology in Lausanne describe an experiment in which players participated in short debates with another human and a GPT-4 model that was given additional information about the opponent, such as age, employment, and political affiliation. They found that the personalized GPT-4 model was 82% more persuasive than the human<sup>71</sup>. The researchers state that AI models “are typically significantly more effective at logical and analytical reasoning than humans”. They suggest that the next step in the development of these models could be “spy” AI, in which LLMs can perform actions on the user’s behalf. As if to confirm its findings, the Alan Turing Institute recently tested LLM\_OSINT, a model that allows for the construction of a dossier on a specific individual using open sources, developing their psychological profile, answering their questions, and writing persuasive phishing emails. Combining this model with others, one could imagine a virtual intelligence agent handling every stage of the intelligence process, including agent recruitment<sup>72</sup>.

In summary, new technologies have and will continue to have a profound impact on intelligence operations in every area of their operations. However, as

<sup>70</sup> J. Lawless, *Britain’s MI6 intelligence chief says AI won’t replace the need for human spies*, <<https://www.independent.co.uk/news/richard-moore-ap-britain-mi6-russia-b2377898.html>> (19.06.2023).

<sup>71</sup> E. Naprys, *GPT-4 is 82% more persuasive than the average human*, <<https://cybernews.com/tech/gpt4-more-persuasive-than-human/>> (02.04.2024).

<sup>72</sup> A. Janjeva, A. Harris, S. Mercer et al. *op. cit.*

this publication points out, in certain areas of intelligence activity and in certain situations, it is beneficial to utilize „old”, proven „espionage” methods, perhaps enhanced with technological advancements.

## BIBLIOGRAPHY

1. *12 Months of Fighting Cybercrime & Defending Enterprises | SentinelLABS 2024 Review*, <<https://www.sentinelone.com/blog/12-months-of-fighting-cybercrime-defending-enterprises-sentinelabs-2024-review/>>
2. Appel E.J., *Cybervetting: Internet Searches for Vetting. Investigations and Open-Source Intelligence*, Second Edition, CRC Press 2014
3. *Artificial intelligence can speed-sort satellite photos*, “The Economist” <<https://www.economist.com/technology-quarterly/2024/07/01/artificial-intelligence-can-speed-sort-satellite-photos>>
4. *Artificial intelligence can speed-sort satellite photos. Could it also recruit an agent?*, <<https://www.google.com/search?client=firefox-b-d&q=Artificial+intelligence+can+speed-sort+satellite+photos>>
5. Bateman A., *Mutually assured surveillance at risk: Anti-satellite weapons and cold war arms control*, “Journal of Strategic Studies” 2022, Vol. 45, No 1, Published online: 26.01.2022
6. Brzeziński D., *Top modeling*, Politechnika Poznańska Instytut Informatyki, <[https://www.cs.put.poznan.pl/alabijak/emd/11\\_Topic\\_modeling.pdf](https://www.cs.put.poznan.pl/alabijak/emd/11_Topic_modeling.pdf)>
7. *CIA agents tracked by technology in 30 countries*, <<https://nexusnewsfeed.com/article/geopolitics/cia-agents-tracked-by-technology-in-30-countries/>>, access: April 23, 2018.
8. Cole D., *We Kill People Based on Metadata*, <<https://www.nybooks.com/online/2014/05/10/we-kill-people-based-metadata/>>
9. Devost M., *Duyane Norman on Disrupting the CIA to Deal with Emerging Threats*, <<https://oodaloop.com/oodacasts/intelligence/duyane-norman-on-disrupting-the-cia-to-deal-with-emerging-threats/#:~:text=Duyane%20Norman%20spent%20nearly%2030%20years%20in%20the,of%20the%20CIA%20Counterterrorism%20Center%E2%80%99s%20Incident%20Response%20Team>>
10. Dorfman Z., McLaughlin J., *The CIA’s communications suffered a catastrophic compromise. It started in Iran*, Yahoo News, <<https://www.yahoo.com/news/cias-communications-suffered-catastrophic-compromise-started-iran-090018710.html?guccounter=1>>

11. Hendrix J., *Transcript: Senate Hearing Addressing the National Security Implications of AI*, <<https://www.techpolicy.press/transcript-senate-hearing-addressing-the-national-security-implications-of-ai>>
12. Ingesson T., Andersson M., *Clandestine Communications in Cyber-Denied Environments: Numbers stations and radio in the 21st century*, “Journal of Policing, Intelligence and Counter Terrorism” 2023, Vol. 19, No 2
13. Janjeva A., Harris A., Mercer S. et al., *The Rapid Rise of Generative AI. Assessing risks to safety and security*, Research Report Centre for Emerging Technology and Security (CETaS), The Alan Turing Institute 16 December 2023, <<https://cetas.turing.ac.uk/publications/rapid-rise-generative-ai>>
14. Lawless J., *Britain’s MI6 intelligence chief says AI won’t replace the need for human spies*, <<https://www.independent.co.uk/news/richard-moore-ap-britain-mi6-russia-b2377898.html>>
15. *Matt Blaze on OTP Radio Stations*, Posted on September 18, 2020, <<https://www.schneier.com/blog/archives/2020/09/matt-blaze-on-otp-radio-stations.html>>
16. Mason L., Jason M., *Emerging from the Shadows. Redesigning the UK’s security apparatus for a more prosperous future*, CETaS Expert Analysis 28 November 2023
17. Milenkoski A., Vögele J-F., *ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware*, <<https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/>>
18. Naftali T. J., Masoud T. E., *Transcript. Interview with Robert M. Gates. George H. W. Bush Oral History Project*, College Station, Texas, <<https://millercenter.org/the-presidency/presidential-oral-histories/robert-m-gates-deputy-director-central>>
19. Naprys E., *GPT-4 is 82% more persuasive than the average human*, <<https://cybernews.com/tech/gpt4-more-persuasive-than-human/>>
20. NBC News: *Former CIA officer says traditional spying is ‘dead’ due to technology, internet*, <<https://www.yahoo.com/news/former-cia-officer-says-traditional143030382.html>>
21. *Open source intelligence is piercing the fog of war in Ukraine*, “The Economist”, <<https://www.economist.com/interactive/international/2023/01/13/open-source-intelligence-is-piercing-the-fog-of-war-in-ukraine>>

22. *Private firms and open sources are giving spies a run for their money*, The Economist Report: Watching the watchers, <<https://www.economist.com/technology-quarterly/2024/07/01/private-firms-and-open-sources-are-giving-spies-a-run-for-their-money>>
23. *Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools*, <<https://cloud.google.com/blog/topics/threat-intelligence/ransomware-attacks-surge-rely-on-public-legitimate-tools>>
24. Schoenegger P., Park P.S., Karger E. et al., *AI-Augmented Predictions: LLM Assistants Improve Human Forecasting Accuracy*, <<https://arxiv.org/abs/2402.07862>>
25. Shashank J., *How private intelligence companies became the new spymasters*, <<https://engelsbergideas.com/essays/private-intelligence/>>
26. *Signals intelligence has become a cyber-activity*, <<https://www.economist.com/technology-quarterly/2024/07/01/signals-intelligence-has-become-a-cyber-activity>>
27. *Stories of Spycraft: Former CIA Chief of Station John Sipher on Russia and Clandestine Services*, <<https://www.bing.com/videos/riverview/relatedvideo?q=John+Sipher%2c+a+former+CIA+station+chief+in+Moscow>>
28. Strzok P, *Compromised: Counterintelligence and the Threat of Donald J. Trump*, Houghton Mifflin Harcourt 2020.
29. Surdyk K., *OSINT w epoce Wielkich Zbiorów Danych (Big Data)*, „Przedsiębiorstwo Przyszłości” 2022, No 3 (52)
30. Tomlinson R., *The Big Breach: From Top Secret to Maximum Security*, Global Pr 2001
31. *UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion*, <<https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion>>
32. *Vision for the IC Information Environment An Information Technology Roadmap*, <<https://www.dni.gov/files/documents/CIO/IC-IT-Roadmap-Vision-For-the-IC-Info-Environment-May2024.pdf>>
33. Ларина Е., Овчинский В., Как изменилась разведка в мире технологий, <[https://zavtra.ru/blogs/kak\\_izmenilas\\_razvedka\\_v\\_mire\\_tehnologij](https://zavtra.ru/blogs/kak_izmenilas_razvedka_v_mire_tehnologij)>