# An Introduction to Intelligence Studies

12 Apr 2020

**Summary**
Intelligence Studies deal with the question what Intelligence Services do, how they do it and why. They can be responsible for the civil and/or the military sector and be focused on internal (homeland) or external (foreign) affairs. A key activity is information gathering, but they may also be active in Political Warfare and related areas.
This paper provides basic knowledge for anyone who is doing or interested in strategic and security studies.
After an overview on the term intelligence and the topics of intelligence studies, the structure and rationale of intelligence communities and cooperation between intelligence services is presented, followed by a discussion of the legal and political dimension and the relationship to media.
The following section presents covert activities in Political Warfare.
Finally, the new field of cyber espionage and the impact on the structure and activities of intelligence services is briefly presented.

## Contents

# 1. Fundamentals

## 1.1 Introduction

Intelligence Studies deal with the question what Intelligence Services do, how they do it and why. They can be responsible for the civil and/or the military sector and be focused on internal (homeland) or external (foreign) affairs. A key activity is information gathering, but they may also be active in Political Warfare and related areas.

This paper provides basic knowledge for anyone who is doing or interested in strategic and security studies[1].

After an overview on the term intelligence and the topics of intelligence studies, the structure and rationale of intelligence communities and cooperation between intelligence services is presented, followed by a discussion of the legal and political dimension and the relationship to media. The following section presents covert activities in Political Warfare. Finally, the new field of cyber espionage and the impact on the structure and activities of intelligence services is briefly presented.

## 1.2 What is Intelligence?

The term intelligence can be used in different ways. In psychology and neurology, this means the intellectual capacity of an individual. In Intelligence Studies, this refers to information, knowledge and secret services.

However, there is no widely accepted definition of intelligence[2].

Some authors focus on the final product, i.e. the resulting (advanced) knowledge and information while others refer to the process of information gathering and handling.

The **Intelligence Cycle** describes the collection, processing, validation, analysis, discussion and presentation of information as continuous process.

Some authors focus on the information gathering from foreign countries, but in the era of extremism and home-grown terrorism it is apparently necessary to look on the own country as well.

Is Intelligence just another word for secret? Not necessarily, as there can be different forms of intelligence:

- **Human Intelligence (HumInt)**: gathered from human sources
- **Imaging Intelligence (ImInt)**: gathered from pictures, such as satellite images
- **Signals Intelligence (SigInt)**: gathered from telecommunication/digital communication

and

- **Open-source Intelligence (OsInt)**: gathered from publicly available sources.

It is common understanding that the majority of information provided by Intelligence Services is OsInt, but the difference comes from the systematic collection and analysis and the combination with secret information, which is often the missing link between facts, persons and events.

[1] In particular, this paper consolidates and updates intelligence-related topics from earlier publications, see Section 6.2 for details (Cyberwar 2019, Biological Warfare 2019, Attribution of Cyber Attacks 2019, Biothreats and Biodefense 2018, Modern Geostrategy 2017).

[2] For details and official definitions, refer to Warner 2020, p.4-13

Note that in media reports intelligence/espionage organizations are often simply called „Intelligence“, but for clarity, the term „Intelligence Service“ will be used in this paper where applicable.
Intelligence Services are not only responsible for information gathering, but can also be involved in all kinds of covert activities, see Section 3.3.

### *1.3 Intelligence Studies*

In practice, Intelligence Studies are studies of what Intelligence Services do, how they do it and why. There are various academic journals and publications for security and intelligence studies, so everybody could do these studies.
An illustrated easy-to-read introduction of history, methods and tools of espionage can be found in the book of H. Keith Melton *The Ultimate Spy* (German Edition: *Der perfekte Spion*). For Advanced Studies, e.g. the Second Edition of the Reader *Secret Intelligence* could be recommended[3].

Full-time university studies are typically Advanced Studies for fully educated and trained staff from security organizations such as Intelligence, Military and State. In US, where these studies already have a long tradition, a typical entry requirement is an appropriate Security Clearance.

Now, the University of the German Federal Armed Forces (*Bundeswehr*) has set up a new Master Course *Intelligence and Security Studies* showing the modern concept of intelligence with topics like cyber defense and security, intelligence governance and accountability, intelligence collection and analysis, global threats, terrorism, extremism etc.
Neighbored disciplines are e.g. *Security Studies*, such as the Master Course Military Leadership and International Security (*Masterstudiengang Militärische Führung und Internationale Sicherheit)* of the *German Institute for Defence and Strategic Studies (GIDS)* in Hamburg and the Master Course *Military Studies* at the University of Potsdam.

## 2. Intelligence Cooperation

The security sector of a nation state typically consists of multiple organizations such as police, military and intelligence. Intelligence Services may be responsible for the civil and/or the military sector and be focused on internal (homeland) or external (foreign) affairs. In a multipolar world with increasing impact of non-state actors like terrorists and extremists a closer cooperation between organizations is required[4].

What can be done? The standard suggestion is to enhance cooperation between authorities, information exchange between all types and levels, i.e. between secret services, secret

[3] Melton 2013, Andrew/Aldrich/Wark 2020

[4] A thorough discussion of Intelligence Cooperation is done in the book (German language) *Geheimdienste in Europa*, VS Verlag für Sozialwissenschaften 2009

services and other security agencies (police, customs authorities) and to enhance international cooperation as well.
Cooperation can mean organizational and/or financial support and the common collection and exchange of information, e.g. by new databases. Also, coordination centers and coordinators maybe established. However, there are concerns that there has to be a balance between security and privacy, i.e. human rights need to be respected and the appropriateness of actions needs to be carefully controlled.

The system of intelligence cooperation can be sorted into three levels, the intelligence cooperation within one country (**intelligence community**), the widespread bilateral intelligence cooperation and the multinational intelligence cooperation. Many countries have multiple intelligence organizations that cover inner and external security and civil and military issues. There is a never-ending discussion about the optimum size and number of organizations: a single organization may be too large to be controlled, also the potential damage in case of intrusion could be serious and internal communication maybe too cumbersome with the risk of information loss, late reactions and blind spots in analysis. Smaller organizations have specialization advantages and may be more focused on certain topics, but there is a risk of overlapping actions and responsibilities, internal competition and communication issues.

There is a discussion whether intelligence units should share their communication with others. Of course, there may be a competition between units and organizations, but information sharing has an inherent risk of disclosing the source of the information. This may lead to take-over of the source by another organization or interference with the own operations, which increases the risk of mission failure.
A standard solution here is not to provide the **raw intelligence** (source, timepoint, original text), but **assessed intelligence** (providing the information only with an assessment of validity and reliability).

The standard solution for nation state intelligence is to have multiple organizations with a coordinating level[5]. The largest Intelligence Community is in the US (formally established in 1981) where the *Director of National Intelligence DNI* (since 2004 in response to 9/11, his office is known as *ODNI*) coordinates all organizations, 8 of them are forming the military umbrella organization *Defense Intelligence Agency DIA*[6].

[5] Carmody 2005

[6] The 8 DIA organizations are the Air Force Intelligence, Surveillance and Reconnaissance Agency (ISR), United States Army Intelligence Corps (G2), Office of Naval Intelligence (ONI), Marine Corps Intelligence Activity (MCIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO) for satellites, National Security Agency (NSA) for SigInt. Non-military organizations are the Central Intelligence Agency (CIA), Office of Intelligence and Counterintelligence (Department of Energy), Bureau of Intelligence and Research (INR) (State Department), Office of Intelligence and Analysis (OIA) (Department of Finance), Office of National Security Intelligence (NN), Drug Enforcement Administration (DEA), Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), refer to DNI Handbook 2006

The second level is a network of **bilateral intelligence cooperation**, e.g. Germany has relations with more than 100 countries[7]. Depending on quality of political relationship, there may be formal official intelligence representatives and/or as (more or less) accepted alternative, intelligence staff as diplomatic (embassy and consulate) staff. This is necessary to detect, discuss and resolve bilateral intelligence-related incidents and topics.

The highest level is the **multi-lateral cooperation**, because even the largest intelligence organizations have limited human, technologic and budgetary capacities to achieve a global coverage. The information mode is typically as follows[8]:

- **Do ut des** – if you give something, the other one has to give something, too
- **Need to know** – only necessary information is provided; this is also important if the organization is infiltrated or agents are captured by adversaries
- **Third party rule** –an information received from second parties should not be given to third parties without approval
- **Assessed intelligence** – no raw data to protect knowledge on methods and sources.

Based on this exchange logic, smaller groups can easier have deeper cooperation. US has established already after World War II the declassified **5-eyes** cooperation with UK, Canada, Australia and New Zealand and in response to 9/11 (officially not confirmed, reported in 2013 by *The Guardian* and others in November 2013) a wider cooperation the **9-eyes** cooperation including Denmark, France, Netherlands and Norway and the **14-eyes** cooperation additionally including Belgium, Italy, Spain, Sweden and Germany[9].
When looking on the map, this arrangement reflects not only a preference order, but also a geographical logic. The 9-eyes partners are located at the Eastern and Southern flank of the United Kingdom, while the 14-eyes group are the surrounding neighbors of the 9-eye states, forming together a territorial block. This allows establishing a European platform and to protect surveillance and physical presence in these countries.

In the European Union, cooperation started with small counter-terrorist working groups in the 1970ies and was stepwise expanded. The *Joint Situation Center SitCen* (which since 2010 is subordinated to the *Standing Committee on operational cooperation on internal security COSI*) is analyzing information provided by member state organizations, counter-terrorist working groups etc. [10]
Meanwhile, the *SitCen* is part of the *European External Action Service (EEAS)* and now called *Intelligence Center (IntCen),* which according to the latest Org Chart from 01 Feb 2019 is organized in 4 units *IntCen 1-4* for analysis, OsInt; situation room and consular crisis management. Also, the EEAS has an internal security service for the security of the EEAS itself[11]. The Military Intelligence is coordinated in the *EU Military Staff (EUMS)*. The European intelligence is also cooperating in the *CdB (Club de Berne)* since 1972[12].

[7] Daun 2009, p.72
[8] Jäger/Daun 2009, p.223
[9] See e.g. Shane 2013, p.4
[10] Scheren 2009
[11] Tagesschau online 2019
[12] Scheren 2009

Africa has established the multinational cooperation *Committee of Intelligence and Security Services of Africa CISSA* as a part of the African Union.

# 3. Intelligence Governance

## *3.1 Law and Intelligence*

Political reality is often not black or white, but dirty grey: everybody is doing espionage, but is unhappy if the others do the same.

There is no formal United Nations Convention with respect to espionage, but it is evident that the national laws are logically not consistent when defining the same activity as legal (in a 'good' moral sense) when done by its own people, but as illegal (in a 'bad' moral sense) when done by others[13].

The dilemma is overcome by the customary international law, which accepts the right of sovereign states to conduct espionage. This legal status is the basis for the above-mentioned intelligence cooperation and also for the presence of foreign intelligence officials as legal representatives for discussion, mitigating and resolving intelligence issues.

However, while the espionage as such is an accepted activity of nation states, things are different on the individual level. Often, espionage requires illegal activities, e.g. in cyber espionage, the spies betray users, breach into networks and steal data.

The normal expectation would be that spies, if a nation states takes note of them, are punished in accordance to the national laws. But the reality is that the handling of espionage and spies primarily depends on political and operational considerations and not on legal ones.

For example, states sometimes tolerate espionage activities temporarily as this allows to observe and analyze the tactics and methods of the foreign intelligence, helps to identify the areas of interests and potential targets and finally it can be detected if own citizens are willing to cooperate with a foreign intelligence.

If the states decide to intervene, this can be done in very different ways:

- the spy may be urged to leave the country on short notice
- depending on the diplomatic status, the person can be detained and/or used for exchanges of agents
- the spy may be utilized as double agent, i.e. officially work for one intelligence, but in reality, for another one that uses the agent e.g. to place misleading information and traces or to destroy espionage networks

Of course, the extent and severity of discovered espionage is also relevant, but is apparently not the only decision criterion.

[13] Radsan 2007, p. 623

It is global standard that nation states embed their intelligence activities into a legal framework which defines structure, goals and allowed methods of espionage (e.g. interception).
While it easy to define and allow defensive measures, the use of offensive measures is more complicated. The practical question is for the lawmakers, what spies are allowed to do e.g. against terrorists and in foreign countries, while the intelligence services are in particular concerned what happens if something goes wrong.

A widely established solution for this problem is a **legalist-bureaucratic** intelligence culture. This means that the intelligence service pay attention that their activities are at least formally compliant with the regulations and instructions and that in case of risky operations, all possible options were carefully weighed upfront. This requires review, approval and documentation procedures.

Apparently, terrorists have no problems with law violations, so there is a never-ending discussion whether intelligence procedures are too cumbersome and too slow to react quickly to emerging threats.
On the other hand, lawmakers need to make sure that activities are in line with regulations. As in addition nation states have different intelligence philosophies ranging from pure information analysis to *last line of defense* approaches, there is no objective solution for this problem.

The best that lawmakers and intelligence can do is to understand intelligence regulation as something dynamic which requires a regular and frequent (re)evaluation of both the legal framework and intelligence activities to identify any obstacles and gaps and the willingness to adapt regulations and practice quickly, whenever needed.

## 3.2 Relationship to Media and Politics

Politicians need intelligence services for various reasons, e.g. defense against external threats and espionage, as early warning system, for informed decision making and also for covert activities against adversaries[14].
At the same time, politicians may be concerned that intelligence activities may result in risks for freedom and privacy. A standard solution is to establish oversight by a parliamentary committee which regularly reviews the activities. However, the need for transparency has to be carefully weighed against the need of secrecy.

Information is power, thus not only the government, but also intelligence services form power centers. Strong intelligence laws may allow politicians to control the population, but it can always happen, that the control and surveillance turns against them, i.e. does the government control the Intelligence or vice versa? The phenomenon that the factual power may shift from government to formal or informal security and intelligence communities is described in literature as **deep state**.

[14] For a practical case study of oversight and accountability, see Phytian 2020.

This can also be a reason to form intelligence communities instead of a single service, because multiple competing services represent a balance of power.

However, intelligence services may also be concerned. A historic example provides implications which could be still relevant for modern democratic states.
In a final analysis from 2003, leading intelligence officers from the former Communist German Democratic Republic analyzed the collapse of the German Democratic Republic[15]. One key question was: The *Ministerium für Staatssicherheit MfS* (Ministry of State Security, also known as *Stasi*) was one of the tightest and most effective Intelligence Services in history of Intelligence Studies. Why couldn't they prevent the collapse of the Communist rule and the state?

In short, there was an unrest in June 1953 against the Communist rule. While the MfS and the Soviet Allies argued that the rapid formation of Armed Forces, the so-called Kasernierte Volkspolizei KVP, had overstretched the capacities, the Communist Party SED argued that this was a fascist coup. When the MfS could not provide the evidence for a coup, it was administratively downgraded for some years what definitely affected the relationship between Intelligence and Politicians.
When in the 1980ies the Communist economies were in crisis, the politicians noted the growing problems and requested the MfS to expand surveillance, even up to sports events. When the end came closer, the MfS alerted the government that there is urgent need for reforms. The politicians rejected this as takeover of Western propaganda. A few months later, the Communist rule, the MfS and the state collapsed.

Conclusions:

- Even total control and information is futile, if the politicians are not able or willing to draw the necessary conclusions from the provided information.
- Politicians must be able to accept unpleasant truths and should take intelligence reports seriously.
- Intelligence can only detect and analyze political problems, but cannot solve them instead of politicians.
- An intelligence service which has to focus on everything has at the end no focus anymore.

Also, the relation between journalists and intelligence is complex, but in some ways similar to the general relationship between politicians and journalists[16].
Intelligence Services need journalists e.g. for transfer of information, such as raising public awareness for cyber espionage or other security-related topics (because which average citizen regularly would visit intelligence websites?).
On one hand, journalists may be concerned that they could be used as tools of information warfare. States may use intelligence to observe critical journalists, but also to gather background information as some journalists have access to strategically relevant sources[17].

[15] Grimmer et al 2003 p.I/44-239
[16] Bannas 2018, p.10
[17] Müller 2019b, p.8

On the other hand, journalists/media may function as watchdog substitutes[18] or may unveil leaks and scandals which could result in disclosure of confidential information and operations.

To overcome uncertainties and the risk of bad surprises, both sides have developed strategies:
Intelligence Services try to establish working relationships to trusted journalists by background talks[19] while on the other side leading newspapers employ experienced journalists who are specialized on security and intelligence topics. As a result, both sides know then what they can expect from each other.

## *3.3 Political Warfare*

### 3.3.1 Introduction

The concept of Political Warfare as it is used today was formulated in the US in 1948 and is still dominant in the respective research literature, so this section primarily refers to the US example.
**Modern Political Warfare** is the employment of all overt and covert means to achieve its national objectives and consists of the intentional use of one or more forms of power - diplomatic/political, information/cyber, military/intelligence, and economic- to affect the political composition or decision-making in another state. This is ranging from psychological measures up to short of war-activities[20].
The difference to conventional policy making is the **focus on enforcement**, e.g. use sanctions instead of trade, active support of regime changes instead of criticizing other states etc., targeted use of information and actions as psychological warfare and so on.
Political Warfare ranges from overt actions as political alliances, economic measures (aid, sanctions, sabotage), and "white" propaganda to covert operations as clandestine support of "friendly" foreign elements (parties, persons, NGOs), "black" **psychological warfare** (also known as **PSYOPs**), and **unconventional warfare (UW)** as support of a foreign insurgency or resistance movement against its government or an occupying power. In practice, these aspects are typically handled as a matter of **Special Operation Forces (SOF)** and as **Support-to-Resistance (STR)**[21].
Friendly states can be supported and defended by **Nation Assistance**: programs include **security assistance (SA), humanitarian civic assistance (HCA)**, and **foreign internal defense (FID)**, i.e. **counterinsurgency (COIN)**.

Modern Political warfare has certain characteristics[22]:

[18] Hillebrand 2020
[19] Müller 2019a, p.8
[20] Note that there is a discussion whether the use of kinetic force (military or paramilitary force) should be separated from political warfare as hybrid warfare (Babbage 2019, p.1). However, both from the history of this concept (Kennan 1948) and practice of the Support-to-resistance operations (Irwin 2019, p.x), this approach may be a bit too narrow.
[21] For terminology which is used in US military, refer to Searle 2017, in particular to chapter 4 Implications of the Theory for Conventional and Special Operations.
[22] RAND 2018 and 2019

- It extends conventional forms of political conflicts instead of replacing them.
- It is outside traditional warfare, the aim is "*winning without fighting*" [23], but can be done in parallel to traditional warfare.
- Typically, it is a combination of activities which require intelligence support to ensure precision and to prevent detection and attribution by the target state.
- In open conflicts, economic pressure as the preferred tool of the strong can be exerted.
- At each stage, information warfare can be used as targeted amplification or obfuscation of information in combination with cyber activities.
- The use or targeting of non-state actors and organizations is included.
- Religious, ethnical and other societal divisions of the target states may be used to improve effectiveness.

### 3.3.2 Information Warfare

The concept of information warfare is well established, e.g. in psychological warfare, targeted information or propaganda was released to adversaries to influence their behavior. The modern information warfare is a bit different, as this is the *combined manipulation of digital technologies and information* to influence adversaries.

In summer 2017, a study about **computational propaganda** was published by the University of Oxford[24]. The authors define computational propaganda *„as the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks"*. Currently, *Facebook* and *Twitter* are the main platforms for those activities.
The EU has established a task force which should detect **fake news**, to correct them and also should support a positive perception of the EU in Eastern States[25].

Information can be used as political weapon. In the past, this was called (referring to Russian term) **Kompromat**, which included real and/or fabricated facts about political adversaries to weaken them.
A modern version are **Leaks**, which can be done by state or non-state actors. While initially leaks were typically released in Internet, meanwhile also intercepted or recorded confidential telephone calls from leading politicians are published.

### 3.3.3 Special Forces

The use of Special Forces and active physical force is not only a question of political motivation, but also of capacities. Thus, such activities are typically considered only by larger countries.

[23] Babbage 2019
[24] Woolley/Howard 2017
[25] Stabenow 2017, p.3

The **Special Operations** and the **Support to Resistance (STR)** were originally invented by the World War II US military intelligence OSS which was later on replaced by the modern intelligence community.
The intelligence branch of special operations is the *Central Intelligence Agency (1947)* which is organized as follows: The *Special Activities Center (SAC)* is a division of the CIA responsible for covert operations, since 2015 known as *Special Activities Division*. Within SAC there are two separate groups: *Special Operations Group (SOG) for tactical paramilitary operations* and *Political Action Group (PAG)* for covert political action related to political influence, psychological operations, and economic warfare.
The military branch is the *US Army Special Forces* (1952), other agencies have limited capacities as well, i.e. the *Drug Enforcement Agency DEA*.
**Special Operation Forces (SOF)** are doing different, unusual things and Special Operations are e.g. applied in unusual situations such as covert operations and may thus require direct cooperation with members of intelligence, police or justice authorities[26].
The **Support to Resistance (STR)** concept involves the synchronized planning and execution of a series of activities that require close collaboration across US Government departments and agencies, e.g. between the *Department of Defense*, the *State Department* or the *Central Intelligence Agency (CIA)*, and there may be a shift in the lead responsibility over the course of the operation[27]. This may include the use of Special Operations and Special Operation Forces. STR can serve as a tool of disruption, of coercion and to enable regime change and can be done during wars or in peacetime.

# 4. Cyber Espionage

## *4.1 Brief Introduction*

Cyber attackers are the so-called hackers, who look for vulnerabilities in programs and systems and then take control with their own programs such as viruses or Trojans. They try to persuade users by social engineering and phishing to open malicious attachments or websites, to disclose passwords and account information.
There are 4 main targets, namely the normal users, the private sector, the state with politics, administration and public institutions, and the critical infrastructures that are needed for life, such as electricity and water supply, hospitals, etc.
Criminals represent the most frequently acting attacker group, then Intelligence Services, while terrorists and cyber armies have so far barely appeared.
Criminal hackers steal data to sell or exploit the victim's account. Or they use screen blockers (ransomware) to request money for the removal. Sometimes they also use the computers to attack other victims or to create digital money (bitcoin or crypto mining).
Intelligence Services can use hacker teams, so-called **Advanced Persistent Threats (APTs)**, which are active in politics, business and technology, including sabotage. Foreign governments and administrations are always interesting and under constant espionage

[26] Searle 2017, p.23
[27] Irwin 2019

pressure, while normal users are less in focus because it is difficult to filter out something useful from the mass (the needle in the haystack).

The hackers of industrial espionage loot research institutions, high-tech and armaments companies. Sabotage hackers attack factories and critical infrastructures, which has already led to power outages. Among other things, they can disrupt productions, delete data and damage digital devices or directly the computer chips.

## *4.2 Advanced Persistent Threats*

The leading hacker groups are also referred to as **Advanced Persistent Threat (APT)**. The classic definition defines APTs are longer-term attacking groups with defined **techniques, tactics and programs (TTPs)**.

Recent years have shown that an APT is a project group within an intelligence unit that develops and applies its TTPs and targets along the operational goals of the intelligence unit. APTs do not self-evolve, they are formed by putting together appropriate people and aligning their cyber activities to the operational goals.

APTs are typically characterized by the efforts and complexity of the used tools, the need for specialists to maintain and hide the operations sometimes over several years, to select victims of high political and strategic relevance, to collect and analyze the gathered information and so on. Also, these attacks are typically cases where no immediate profit can be expected, in contrast to cyber criminals who could make money with banking trojans, ransomware etc.

Additionally, each group has its characteristic combination of access vectors, exploits/vulnerabilities, and toolkits which allow differentiation between groups[28]. As each group has a typical set of attack targets, the logic of target selection is also called **victimology**.

## *4.3 Espionage Malware*

Sophisticated espionage malware is increasingly used and the conventional differentiation between viruses, worms and Trojans is becoming less relevant.

Typically, a malware program consists of two parts, an infection part, that installs the program on a computer and other parts that contain the instructions of the attacker. Meanwhile, it is practice to install a small initial **backdoor program (beachhead)** and to install further parts later that may also allow expanding administrator rights on the infected computer.

Examples for such programs are **keyloggers**, which report any pressed key to another computer which allows to overview all activities and also to register all passwords and **rootkits**, which are tools that allow logins and manipulations by the attacker without knowledge of the legitimate user.

To avoid detection, the malware conducts **self-encryption** steps and may have a **self-deletion** module for the time after completion of espionage. Ideally, this includes the option for **self-deactivation** (going silent). Then, further malware elements are imported based on the initial information gained. Instead of creating large malware programs, now variable

[28] See also Jennifer 2014

**modules** are uploaded that are tailor-made for the target user and the digital environment. The most advanced malware has a more or less total control of the infected computer and can extract all kind of data. Storage of malware and information is done at uncommon places such as the registry or even in the firmware to avoid detection and removal from the computer. A typical operational step is to escalate unprivileged users to administrator right to gain network control (**lateral movement**). This results in an **Advanced Persistent Threat (APT)**, i.e. the access by unauthorized persons to a network and to stay (persist) there for a longer time.

## *4.4 Contractors and Insider Threats*

The most significant leaks of Intelligence Information came from Insider Leaks and not from hackers, i.e. people with regular access to the information who made an unauthorized release of this information.

Typically, these leaks came from private **contractors** from security partners of the affected intelligence organizations[29], i.e. external employees. It is meanwhile standard that large intelligence communities have **security partners**, i.e. private companies who provide additional workforce for intelligence-related duties.

The **privatization of intelligence** (which is also relevant for the creation of cyber weapons and cyber espionage programs) has the advantage of more flexibility and quicker adaptation to evolving threats. This creates however new vulnerabilities which are not under direct control of the intelligence services. These uncertainties may be reduced by a long-standing security cooperation with firms who provide services or contractors to support the state organizations. On the other hand, insider threats could also result from regular internal employees of the intelligence services.

Defense strategies can be focused on the information access and flows, but also on the individuals.

Possible countermeasures against insider threats (but also against external attacks) could be **vertical segmentation** based on ranks and **horizontal segmentation** of access depending on project-related or topic-related involvement, blockade of printing and downloads by **document management** systems and the **tracking** of document usage and changes. Also, the transmission of confidential data via secured or physically **separated communication** lines in line with the **need to know-principle** may help to prevent further security incidents[30]. Also, the regular review and minimization of access rights is necessary.

On the individual level, the initial **security clearance** procedure could be expanded to an overall **integrity check**, i.e. evaluating whether the personality and psychological condition of such a person makes them eligible for their position. Repeat checks could e.g. be triggered by unexpected changes of behavior or lifestyle (which both may indicate takeover and payment by an adversary). In case of critical incidents, also questionings with polygraphs are still an option[31].

[29] For details, refer to Cyberwar 2019 in Section 6.2

[30] Sattar et al. 2010, p.3

[31] Shane/Perloth/Sanger 2017

## *4.5 Relation between Conventional and Cyber Intelligence*

One key question for a cyber-attack is: who did it? Attribution is the allocation of a cyber-attack to a certain attacker or a group of attackers in a first step and to unveil the real-world identity of the attacker in a second step. While the methods of attacker allocation have made significant progress in the recent years, digital technologies often still do not provide definite evidence for the real-world identity of an attacker.

The situation is different if attribution is handled as a **cyber-physical process**, i.e. as combination of digital forensics with evidence from the physical world. Bits and bytes are not really virtual, but still bound to a physical infrastructure which opens different ways to detect adversaries (analysis of physical information flow).

Gaps can also be filled by human intelligence, i.e. conventional espionage. As already happened, for example the simple buying of information (IP addresses) from members of the adversary intelligence can solve the attribution problem.

Also, there is an ongoing discussion, whether cyber intelligence may be a less risky, remote and cheaper way to do the espionage, but cyber espionage can only complement conventional espionage work and cannot replace the presence of local agents.

On the organizational level, the rapidly expanding cyber sector had massive impact on size and structure of intelligence organizations.

Typically, states start managing cyber matters with setting up cyber authorities. In a second step, new matters are addressed with setting up further authorities which then leads to overlapping or unclear responsibilities. The final step is then restructuring and centralization.

A good example is Germany where the originally conventional intelligence services BfV, BND and MAD are now accompanied by a growing number of specialized cyber intelligence units:

Civil sector:

*Federal Ministry of the Interior (Bundesministerium des Innern BMI)* with

- *Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik BSI)* for protection of government IT infrastructure
- *"Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITIS), i.e. Central Service for IT in the security sector* for decryption services (BSI acts as code maker, *Zitis* as code breaker).[32]
- *Agency for cyber security innovations (Agentur für Innovation in der Cybersicherheit)* as civil-military cooperation between ministries of the Interior BMI and of Defense BMVg[33].

Military sector:

- *Cyber and Information Space Command (Cyberinformationsraumkommando CIR)* with *German Army Secret Service for Exterior Affairs (Kommando Strategische Aufklärung KSA)* with the sublevels for electronic warfare, *cyber network operations (CNO)* and the satellites (with the whole *Geoinformation GeoBw*).

[32] Kirchner et al. 2017, p.5

[33] BMI 2018

Intelligence sector:

- Germany's foreign intelligence agency (*Bundesnachrichtendienst BND*) with a department for cyber operations[34]
- Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz BfV*) for domestic intelligence
- *Military Counterintelligence Agency (Militärischer Abschirmdienst MAD)* for the protection of the German army

## 5. Concluding Remarks

The key challenge for students of Intelligence Studies is to handle the ambiguities and blurs of this matter. Intelligence Communities and Cooperation are complex systems of checks and balances and also the relationships to the legal framework, the politicians and the media can be complicated.

However, it was shown that a practical approach to mitigate these problems is the willingness of the various actors to communicate and cooperate. At various instances, strategies for reduction of uncertainties were presented in this paper.

The cyber espionage section has shown that neither the security and intelligence law nor the structure of organizations are set into stone, but are dynamic systems which require frequent (re)evaluation and adaptation.

[34] Mascolo/Steinke 2019, p.9

# 6. Literature

## *6.1 Literature References*

Andrew, C., Aldrich, R.J. and Wark, WW (eds): Second Edition of the Reader Secret Intelligence Routledge 2020

Babbage, R. (2019): Winning without fighting – Chinese and Russian Political Warfare Campaigns and how the West can prevail. Volume II: Case Studies Center for Strategic and Budgetary Assessments CBSA 2019

Bannas, G. (2018): Im Quadratkilometer der Macht. Frankfurter Allgemeine Zeitung, 31 Mar 2018, p.10

BMI (2018): Bundesministerium des Innern (Federal Ministry of the Interior): Agentur für Innovation in der Cybersicherheit. 29 Aug 2018

Carmody, N.F. (2005): National Intelligence Reform. USAWC Strategy Research Report. US Army War College.

Daun, A. (2009): Die deutschen Nachrichtendienste. In: Geheimdienste in Europa. Transformation, Kooperation und Kontrolle VS Verlag für Sozialwissenschaften.

DNI Handbook (2006): An overview of the United States Intelligence Community 2007. Published 15 December 2006

Grimmer, R., Irmler, W., Neiber, G., Schwanitz, W. (2003): Sicherheitspolitik der SED, staatliche Sicherheit der DDR und Abwehrarbeit des MfS. In: Die Sicherheit – zur Abwehrarbeit des MfS, Book 1 of 2, p.44-239, edition ost

Hillebrand, C. (2020): The role of news media in intelligence oversight. In: Andrew, C., Aldrich, R.J. and Wark, WW (eds): Second Edition of the Reader Secret Intelligence Routledge 2020, p. 396-412

Irwin, W. (2019): Support to Resistance: Strategic Purpose and Effectiveness Will Irwin Foreword by Lieutenant General John F. Mulholland, Jr. JSOU Report 19-2. Joint Special Operations University April 2019 ISBN 978-1-941715-37-6

Jäger, T, Daun, A. (2009): Intelligence in der EU. In: Geheimdienste in Europa. Transformation, Kooperation und Kontrolle VS Verlag für Sozialwissenschaften, p.213-239.

Jennifer (2014): Breaking the Code on Russian Malware. The Recorded Future Blog Posted in Cyber Threat Intelligence 20 Nov 2014

Kennan, G.F. (1948): Policy Planning Staff Memorandum 269, Washington, D.C.: U.S. State Department, May 4, 1948

Kirchner, T., Mühlauer, A. und Steinke, R. (2017): Hacken und doch nicht gehackt werden. Süddeutsche Zeitung No. 213, 15 Sep 2017, p.5

NSABB (2009): Enhancing Personnel Reliability among Individuals with Access to Select Agents. May 2009

Mascolo, G., Steinke, R. (2019): Lizenz zum Löschen. Süddeutsche Zeitung No. 109, 11/12 May 2019, p.9

Melton, K.H. (2013): Der perfekte Spion (German edition of *The ultimate spy*). coventgarden, Dorling Kingsley Limited, London, 2013

Müller, R. (2019a): Das Ende des Hintergrundgesprächs? Frankfurter Allgemeine Zeitung, 20 Sep 2019, p.8

Müller, R. (2019b): Das Ende der Aufklärung? Frankfurter Allgemeine Zeitung, 18 Dec 2019, p.8

Phytian, M. (2020): The British experience with intelligence accountability. In: Andrew, C., Aldrich, R.J. and Wark, WW (eds): Second Edition of the Reader Secret Intelligence Routledge 2020, p.376-395

Radsan, A.J. (2007): The Unresolved Equation of Espionage and International Law. Michigan Journal of International Law Volume 28, Issue 3, p. 596-62

RAND (2018): Modern Political Warfare - Current Practices and Possible Responses from Linda Robinson, Todd C. Helmus, Raphael S. Cohen, Alireza Nader, Andrew Radin, Madeline Magnuson, Katya Migacheva RAND Corporation RR1772

RAND (2019): The Growing Need to Focus on Modern Political Warfare (2019) RAND Corporation RR10071

Sattar, M., Löwenstein, M., Carstens, P. (2010): Vertrauliches, Geheimes und streng Geheimes. Frankfurter Allgemeine Zeitung No.279/2010, p.3

Scheren, M. (2009): Vernetzte Sicherheit – Zusammenarbeit der Inlandsnachrichten- und Sicherheitsdienste in Europa. In: Geheimdienste in Europa. Transformation, Kooperation und Kontrolle VS Verlag für Sozialwissenschaften, p.168-181.

Searle, T. (2017): Outside the Box: A New General Theory of Special Operations JSOU Report 17-4 Joint Special Operations University July 2017. ISBN 978-1-941715-20-8

Shane, S. (2013): No morsel too small for a US spy agency. New York Times International 8 Dec 2013, p.1/4

Shane, S., Perloth, N., Sanger, D.E. (2017): Security Breach and Spilled Secrets have shaken the NSA to its core. New York Times online 12 Nov 2017

Stabenow, M. (2017): Warnung in roten Lettern. Frankfurter Allgemeine Zeitung 25 Jan 2017, p.3

Tagesschau online (2019): Spionage im Steakhaus? Tagesschau online 09 Feb 2019

Warner, W. (2020): Wanted: A definition of Intelligence. In: Andrew, C., Aldrich, R.J. and Wark, WW (eds): Second Edition of the Reader Secret Intelligence Routledge 2020, p.4-13

Woolley, SC, Howard, PN. (2017): Computational Propaganda –worldwide– Executive Summary. Working Paper No. 2017.11 University of Oxford, Project on Computational Propaganda 2017, 15 pages

## 6.2 Further Readings

2017 Modern Geostrategy - Methods and Practice
https://repositorium.ub.uni-osnabrueck.de/handle/urn:nbn:de:gbv:700-2017121216405

2018 A Brief Review of Biothreats and Biodefense
https://repositorium.ub.uni-osnabrueck.de/bitstream/urn:nbn:de:gbv:700-2018010416478/5/Biothreats_and_Biodefense_Saalbach.pdf

2019 Political Warfare
https://nbn-resolving.org/urn:nbn:de:gbv:700-201909181987

2019 Biological Warfare – in Schmidt, T. (Ed.): Encyclopedia of Microbiology (Fourth Edition), pages 520-525 Academic Press Elsevier ISBN: 9780128117361
https://doi.org/10.1016/B978-0-12-801238-3.62160-8

2019 Cyberwar-methods-and-practice
https://repositorium.ub.uni-osnabrueck.de/handle/urn:nbn:de:gbv:700-201907091696

2019 Attribution of Cyber Attacks – Chapter 13 in: Reuter, C. (Hrsg.): Information Technology for Peace and Security, 279-303. ISBN: 9780128117361 Springer Vieweg. Abstract in www.springerprofessional.de/attribution-of-cyber-attacks/16544512