Attribution of Cyber Attacks

Methods and Practice

Working Paper – 17 Feb 2017

Summary

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 *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. Gaps can also be filled by human intelligence.
The paper gives an overview on the current methods and practice of cyber attribution with real-world examples.

Table of Contents

1. Fundamentals

1.1 Introduction

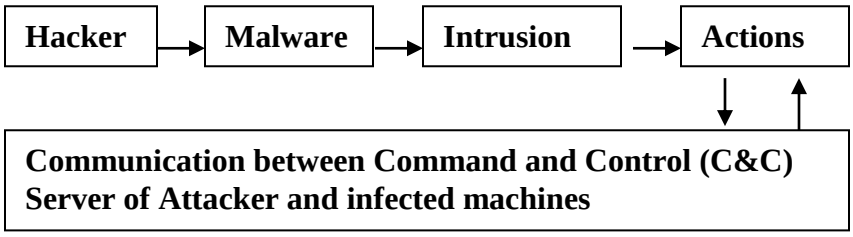
Attribution is the allocation of a cyber attack to a certain attacker or a group of attackers in a first step and to unveil the real-world identity of the attacker in a second step. While the methods of attacker allocation have made significant progress in the recent years, digital technologies often 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. Gaps can also be filled by human intelligence. The paper gives an overview on the current methods and practice of cyber attribution with real-world examples[1].

1.2 Background

1.2.1 Basic principles of cyber attacks

Cyber attacks require the intrusion of the digital device, i.e. the computer, smartphone or all kinds of digital devices with some kind of malware and the communication with the intruded devices to start actions. Dependent on the type of action, the communication will be maintained for a longer time, even for years and complex attacks typically require *bidirectional* communication which gives multiple opportunities for detection and attribution.



Currently, the most frequent and prominent cyber attacks include:

- Malware installation for all kinds of **cyber espionage** (military, politics, industry, finance sector, researchers, international organizations etc.). Sometimes, this is combined with the use of **cyber weapons** such as logic bombs and wiper malware

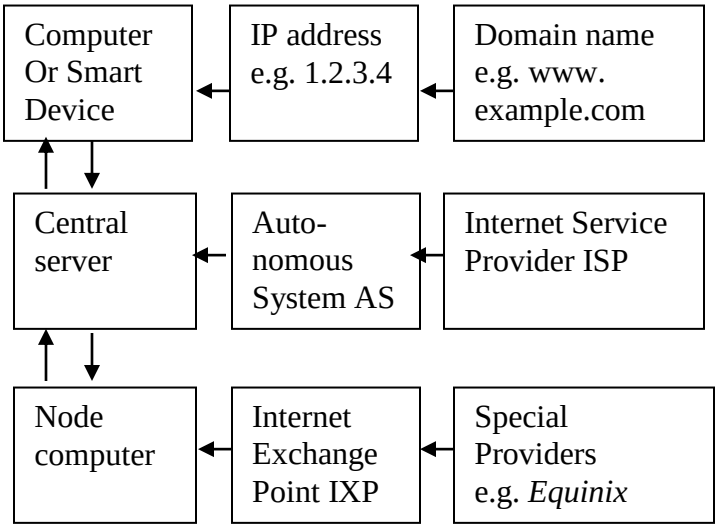
[1] This working paper will strictly focus on the attribution. For background information with respect to intrusion methods, terminology, legal, political and organizational issues as well as of the history of adversary groups you may refer to the free Paper "Cyberwar –Methods and Practice" http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-methods-and-practice.pdf, and the literature cited therein.

- creation of **botnets**, i.e. groups of infected and controlled machines which are misused to send automated and senseless requests a target computer or system which then collapses (distributed denial of service attacks, short **DDoS attacks**). This can be done for political reasons, but also to blackmail the victim as part of cybercrime activities
- Installation of crimeware such as **ransomware** which encrypts the device and the victim is asked for money to get decryption code and banking trojans to gain access to online banking accounts.

1.2.2 Communication lines of cyber attacks

Data, i.e. bits and bytes are not fully virtual, but still have physical representations as a defined electromagnetic condition on storage media and device memory systems[2]. Even wireless transfer results in electromagnetic waves and finally these waves end up physically in devices again. This finding is essential for detection and attribution. As the communication is going via networks of computers, it is helpful to keep the general infrastructure of the internet in mind: This structure also forms the hackers' ecosystem which is presented in next Section 1.2.3.

Simplified model of Internet communication



Typically, an internet communication starts at a certain computer and the data are then transferred to the central computer of an **Internet Service Provider (ISP)**. This central computer is formally known as **Autonomous System (AS)** and large providers may have many of those. However, the Internet Services Providers need to be connected with each other, this is done via node computers, formally known

[2] This sounds trivial, but this means that deleted data on a device are **not erased**. The device only marks the file as 'deleted' and it does not appear on the screen anymore. In reality, the data are still on the storage medium which allows recovery of "deleted" data by forensic and espionage techniques.

as **Internet Exchange Point (IXP)**. In reality, these are large computer centers and not only single computers.

Each computer connected to the internet has an **IP (Internet protocol) address**, a number structured after certain rules. The old 4-digit system of the IP version 4 will now be replaced by larger blocks of the IP version 6, but the principle that a domain is related to an IP address number at a certain timepoint remains the same. This has the same function like telephone numbers for phones, i.e., the technical possibility to connect sender and target correctly.

Now, websites have IP addresses as well, but instead of this normally **domain names** are used, e.g. *www.example.com*. At a certain timepoint, domain names refer to certain IP addresses to avoid communication confusion.

As a consequence, the internet may appear decentralized and virtual in daily routine and it seems almost futile to find out where a cyber attack came from.
In the physical world, the internet is finally bound to a physical network with a significant level of centralization. The US-based company *Equinix* controls with their own IXPs and co-location of client computers in their data centers roughly **90%** (!) of the data volume transfer of the internet[3]. As shown now, this offers opportunities to get insight into the infrastructure of the adversary.

1.2.3 A first step to attribution

Theoretically, a hacker can start a single attack from 'anywhere' and it may be impossible to track this back. On the other hand, the success rate of this approach is quite low.
Attackers who want to achieve significant success are typically attacking on a larger scale, i.e. as groups, with sophisticated malware and act sometimes for years. The longer and the more intense the attack is, the higher the risk for detection and attribution.
Data are incoming and leaving computers via so-called **ports**. A supervisor (IT administrator) can check the ports and the data traffic with commercially available tools. These tools also tell to which IP address the data are or were going.

Now, there are specialized search engines which automatically check what is behind an IP address. An example for such engines is *Robtex.com*. The providers of this service explain on their website that this tool is "*not only"* used by the *National Security Agency NSA*, which indicates that such services also serve as intelligence tools.

[3] Müller 2016, p.7

By entering the IP address in the search mask, *Robtex* shows data flows with other IP addresses as well as the way to the autonomous system AS or the Internet Service Provider ISP. It combines IP addresses and domains as well as any-existing subdomains. Also, it shows mail-servers related to the domain name.

This is important for following reasons:

- Attackers often maintain a certain attack structure, because like any construct an attack environment has both construction costs and exit costs. As a consequence, mail-addresses, domain names, servers and IP addresses are at least partially recycled from one attack to the next. These overlaps allow establishing relations between attacks.
- Attackers need computers as distribution hubs for their malware which results in the use of multiple domain names. Any known domain name may give the way back to the IP address and at the same time forward to the owner of the computer as shown below.

Note that AS computers are numbered along the IANA system and each AS computer is registered. AS computers and the registered persons/organizations can be easily retrieved with further free tools like *ultratools* and many other engines.
For domains and IP addresses, a so-called WHOIS registration exists, often simply available with free search engines. The registration details show company names, addresses, telephone numbers and email-contact addresses. By this, the step from the digital world to the physical world is done, from data to persons and organizations. By this, the researcher may be able to get insight into the 'digital ecosystem' of servers, addresses, registrations, domains etc. of the attacker entity.

Again, even faked registration information is in reality often **re-used** and allows building links between certain attacks. Surprisingly, entering the data into *Google* or any other search engine often leads to further findings which massively increase the chance to find information related to a person with a true real-world identity.

Real world example: In 2013, the Cyber security company *Mandiant* presented an in-depth analysis of Chinese cyber activities and of the APT1 group[4]. Later on, 5 Chinese senior military persons were officially accused by US, including a person assumed to be the hacker with the cover name '*UglyGorilla*'. This person had both a registration of a domain used by APT1 and an available profile as army member. China rejected the accusation, but US media speculated in 2016 that this may have caused the decrease on cyber attacks suspected to come from China in the last two years[5].

[4] Mandiant 2013
[5] Mandiant 2013, Jones 2016, p.5, Nakashima 2016

Further, larger organizations reserve **IP blocks**, e.g. packages of consecutive IP numbers[6]. If a suspected IP address is part of such a block, it can help much to enter all the other IP addresses as well into domain search engines etc.

Real world example: The security researcher *Krebs* was informed about an IP address belonging to the *Carbanak* group which captured 1 billion US-dollars by intrusion of banking systems[7]. His analysis of the IP address registration showed that the company name was also used for past cyber attacks with two different types of malware. The email-address led him to further IP addresses of the *Carbanak* group. The telephone number allowed Mr. Krebs to identify a person with potential relations to the *Carbanak* group, he was even able to have a communication with this person[8].

Note that sophisticated attackers have reacted to this already. One strategy is to exchange IP addresses and servers rapidly with the so-called **fast-flux technology**. Even the shutdown of certain servers can then not stop the attacker. However, a counterstrategy is the use of **sinkhole servers**.
When somebody enters a domain like *www.example.com* into the browser, the computer needs to know the IP address of the target. So-called domain name servers (**DNS servers**) help the computer to find out the IP address.
Sinkhole servers give now intentionally wrong hints (e.g. by saying *www.example.com* is IP address 4.5.6.7 while the true address is 1.2.3.4) and redirect by this the data traffic away from the 'true' computer.
Note that the sinkhole server *can catch* the misdirected data and analyze them. As in larger attacks communication is ongoing for a while, *both* the attacker and the victim data can be collected, which helps to overcome the matter of changing IP addresses. Sinkholing was e.g. used by the Russian security firm *Kaspersky* against the presumably US-based *Equation Group*[9], which on the other hand infected *Kaspersky* with the sophisticated espionage malware *Duqu 2.0* [10].

Real world example: the ransomware-releasing botnet *Avalanche* used the fast-flux technology to avoid detection. Finally, sinkholing allowed catching 130 Terabyte of data. The analysis of this data allowed law enforcement authorities to stop the botnet and to put the *Avalanche* group members into prison. The cooperation of the German *Bundesamt für Sicherheit in der Informationstechnik BSI*, the research unit *Fraunhofer-Institut für Kommunikation*,

[6] There are further technical options, such as giving virtual **IP addresses** within cloud computing and simulating false IP addresses (**IP spoofing**), but in published practical analyses of major cyber crime groups and of Advanced Persistent Threats APT this was not presented as a key issue.
[7] Kaspersky Lab 2015c
[8] KrebsonSecurity 2016
[9] Kaspersky Lab 2015a, p.34-35. Unexpectedly, early versions of Equation Group malware showed hard-coded IP addresses in their programs.
[10] Kaspersky Lab 2015b

Informationsverarbeitung und Ergonomie FKIE, The German Police, Europol, Eurojust, the *FBI* and the security firm *Symantec* made this possible despite the misuse of 800.000 (!) domains[11].

Another strategy is the use of domains with **difficult-to-track registration**, which was 2017 reported by security firm *Kaspersky Labs* for suspected 'survivors' of the *Carbanak* group. Some countries allow the free sale of domains with their country ending, such as Gabon (.ga) by providers such as *Freenom*. However, any provider is at risk to be approached by national or foreign police or intelligence to give access to their data. There is an enormous variability of cyber security laws and law enforcement procedures worldwide, and there is a never-ending public debate and of court cases in the US going on, who under which circumstances is allowed to request information on users from private companies.

The *European Commission Service* released in Dec 2016 an overview on the current legal situation in EU member states. The survey showed an enormous range on the legal perspectives, e.g. whether a provider must or can cooperate, which extent of information is requested, which ways of law enforcement are used (up to remote access to providers) and whether cooperation between authorities is practiced or not[12].
However, the EU is moving towards a common legal framework with a common legal procedure, the **European Investigation Order EIO** and the European Union considers cyber security investigations as an urgent policy matter.

Smart devices have their own IP addresses. The analysis of incidents with smart devices in the Internet of Things (IoT) allows identifying the manufacturer and the involved products.

Real world example: the Internet of Things (IoT) botnet *Mirai* utilized webcams, babyphones and other devices to create a DDOS attack on the US internet infrastructure provider *Dyn* with data flow rates of more than 1 Terabit per second in October 2016. The IP addresses led to the manufacturer *Xiong Mai*.
Some days before, a hacker with the cover name *Anna Sempai* released 62 passwords for access to the devices. Meanwhile, solid evidence was found by security researcher *Krebs* that *Anna Sempai* was involved in the Mirai precursors, in particular *QBot*, while for the *Dyn* attack another group *New World Hackers* claimed responsibility[13].
Later in 2016, the *German Telekom* was massively attacked. Here, a new *Mirai* variant was utilized and analysis showed that again only selected devices (so-

[11] EUROPOL 2016
[12] EU 2016
[13] KrebsonSecurity 2017, Radio Free Europe 2016

called *Speedport* routers) from the Taiwanese manufacturer *Arcadyan* were affected. The attack failed only due to a technical error caused by the malware[14].

2. Hackers

The cyber world can be differentiated into several actor groups:

- The state with civil authorities, military and intelligence organizations. Hackers may work for these organizations, in some states also in state-linked hacking groups.
- Cyber security firms which are involved in detection, attribution and defense, but also in the construction of cyber weapons and espionage tools. Hackers may also act as **penetration testers** to check security measures of a certain unit.
- In the scientific and commercial sector, hackers may work as **White Hat Hackers** to find and to close security gaps, but also as **Black Hat Hackers** for criminal purposes or for industry espionage.
- **Hacktivists** use their skills for political activities.

Please note that the above mentioned spheres are not completely separated. In reality, a skilled hacker may be awarded during a hacking contest, then hired by the state and thereafter switching to the private security sector[15].

While the original image of hackers was more anarchic, meanwhile states are intensely and routinely searching for skilled hackers in order to hire them. **IT summer camps, hacking contests, hackathons** (hacking marathons where a certain problem has to be solved) are typical activities. The search for hackers is however only a small part of the search for skilled IT people in general: Skilled IT students may also be directly contacted by states and security firms. The staff recruitment methods by intelligence and military have made significant progress. Studies have shown that the historical distance between hackers and state organizations has changed to a growing acceptance and interest to work for the state under certain circumstances[16]. As a consequence, recruitment methods for cyber security-related positions are now easier[17].

[14] Alvarez/Jansen 2016
[15] Rosenbach 2016, Kramer 2016
[16] Zepelin 2012, p.27. Krasznay 2010 cited by Chiesa 2012, slide 69.
[17] Zepelin 2012, p.27. The following may illustrate the open approach: When searching since 2012 in US for cyber war issues (search words including the term cyber war) on *startpage.com*, a service allowing anonymous search on Google, it could happen that a sponsored link from the NSA appeared (also visible on *ixquick* or *metacrawler*). This offered cyber careers under the link www.nsa.gov/careers saying "National Security Agency has cyber jobs you won't find anywhere else!". In 2016, this is available under intelligencecareers.gov/nsa. The CIA also set up an own search engine ad "CIA Cyber careers – The work of a Nation – cia.gov The Center of Intelligence –Apply today" and opened in June 2014 an official Twitter account.

The typical hacker is now a younger male person who –if involved into larger cyber attacks- is doing this as a regular job. The dominance of younger males in hacking reflects the dominance of younger males in the IT sector in general. This is meanwhile seen as a problem as this indicates the under-utilization of females for IT. The British cyber intelligence *Government Communication Headquarter GCHQ* is now systematically searching for skilled females by initiating the *CyberFirst Girls Competition* for 13 to 15 year-old girls with tests in cryptology, logic and coding. End of Feb 2017, 600 teams will start the competition. Currently, only 37% of the 12.000 employees in the British Intelligence Sector are females[18].

The typical hacker is not a lonesome rider, but interacts with friends and other hackers to exchange tools and experience, to get insights and news from the scene and so on. This is done with cover names in **hacker fora**, on the **black market** and in the **darknet**[19]. These three areas overlap with each other. Sometimes, **defacement websites** exist where hackers post screenshots of the hacked and damaged (defaced) websites as a kind of trophy.

This opens the way to attribution: cover names may appear in several attacks, also the used email addresses. If an individual hacker makes public claims, the risk of being captured is increased, such as the hacker with the cover name *Anna Sempai* who was involved in the *Mirai* botnet attacks and who is probably identified already[20].
Again, it can be helpful to enter the cover name of a hacker into a search engine to get further clues. Practice shows that hackers sometimes use multiple cover names, but not too many of them, because otherwise they lose their 'profile' in the insider scene.

Real world example[21]**:** In the *Winnti 2.0* attack, a bot communication in *Twitter* used as header the cover name of one of the hackers which also appeared in hacker fora. There, he had email communications with friends who had regular social media websites with all contact details. Also, a short abbreviation in the malware program resulted in further matches in search engines and led to a hacker team, from there to a mail address which then led to a young male person.

The darknet was presented in media in 2016 and 2017 as a major problem. The **TOR system** (derived from *The Onion Router*) is considered my media as the

[18] Wittmann 2017
[19] For an overview refer to Chiesa 2015
[20] KrebsonSecurity 2017
[21] Kaspersky 2013, p.53ff.

backbone of the darknet, because it allows splitting of data packages over multiple routes and by this a high level of anonymity in the net.
However, TOR is increasingly under pressure. A recent paper by the *Naval Research Laboratory* that historically invented the TOR system shows that the takeover of an autonomous system or an IXP node computer (see above in Section 1) by an adversary would provide enough information to capture a user within weeks or sometimes even within days[22]. While this was presented as statistical modeling, it highlights that the TOR system may not be forever a barrier against detection and attribution.

With respect to darknet, one should bear in mind that actors may also be undercover agents[23].

[22] Johnson et al. 2013
[23] Tellenbach 2017, p.31

3. Malware and Advanced Persistent Threats

3.1 Sophisticated malware and hacker units

Meanwhile, several sophisticated hacker units and malware families were discovered and reported which are presented in the following chapters. Typically, it is assumed that these units are linked to or sponsored by states (government/intelligence/military). Reasons for this assumption are 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[24]. A widely used term for this combination is **Tactics, Techniques, and Procedures (TTPs)**. As each group has a typical set of attack targets, the logic of target selection is also called **victimology**.

The attack tactic varies: Leading techniques are **phishing emails** with infected attachments or links to infected websites. As outlined in the *APT28/Fancy Bear* analysis of the Security Firm *FireEye*, such emails can also be used as traces, such as ”specific email addresses, certain patterns, specific name files, MD5 hashes, time stamps, custom functions and encryption algorithms”[25].

Stolen security certificates and the use of **zero-day exploits** are typical indicators for a sophisticated attacker group.

However, assignments to states should be handled with caution. Sometimes, **false flags** are set, i.e. misleading traces to blame another actor, or malware was utilized which is meanwhile known and available on the underground market. In certain cases, cyber weapons are even commercially available with restrictions.

Also, so far no government or authority has ever officially confirmed a link to a hacker unit. A ‘linkage’ to a state is a vague term, this does not indicate that a unit is a formal part of a government organization or only contracted or cooperating.

The below groups are the most prominent units in the media, the total number of larger active hacking groups is estimated around hundred groups.

From the US security analyst perspective, Russia has made significant progress with establishing sophisticated units within the last ten years. While *APT28/Fancy*

[24] See also Jennifer 2014

[25] FireEye 2014, p.29

Bears, APT29/Cozy Bears and *The Waterbug group* are attributed by many analysts to Russia, the links to Russia are still under debate for groups with focus on ICS/industry systems such as *Energetic Bear/Dragonfly* and *Sandworm/Quedagh*[26].
The *Comment Crew/APT1* and the *Axiom/DeepPanda Group* were discussed to be linked with China, while the *Lazarus Group* was assumed to be linked to North Korea. The *Equation Group* is typically assumed to be linked to US, with common reference to the so-called *Snowden leaks*. But please note that all respective governments denied and declined to comment.

All leading groups have multiple names, because analysts typically assign a working name and it appears later that the same group was addressed by different analysts. Also, cyber security firms have internal naming conventions, such as *Bear* = presumably Russian, *Panda* = presumably Chinese and so on. Sometimes, codes or terms in the malware trigger the naming, e.g. the name *Sauron* in the recently discovered APT *Project Sauron* (the all-seeing evil eye from *Lord of the Rings*). It is crucial for attribution to know the alias names to combine knowledge from different sources properly.

Real world examples: *APT 28* is also known as *Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bears* or *Strontium, APT 29* as *Cozy Bears* or *The Dukes*, the *Axiom Group* is also known under as *DeepPanda, Shell_Crew, Group 72, Black Vine, HiddenLynx, KungFu Kittens etc.*

Currently, the most frequently mentioned Cybercrime groups under discussion were the *Carbanak group* and the *Avalanche* ransomware botnet.

3.2 Analysis of Malware

Sophisticated malware can attack, intrude, doing espionage and manipulate computers. This type of software is more and more in use and the conventional differentiation between viruses, worms and Trojans is becoming less relevant. The most advanced types show technical similarities:

Initially, only a small program is loaded which makes intrusion easier. To avoid detection, the malware conducts **self-encryption steps** and creates a **self-deletion** module for the time after completion of espionage. Ideally, this includes the option for **self-deactivation** (going silent). Then, further malware is imported based on the initial information gained. Instead of creating large malware programs, now variable **modules** are uploaded that are tailor-made for the target user and the

[26] See e.g. Jennifer 2014

computing 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. is the access by unauthorized persons to a network and to stay (persist) there for a longer time.

Analysis of malware is impacted by **false flags**, i.e. misleading time stamps and language settings of computer the intruder used for malware creation, in addition, code pieces and terms maybe used that give misleading hints to other attacker groups. Note that this process has a high risk for errors, in larger malware programs it happens that single time stamps were not changed and language settings were not clean enough.
Also, hackers create **digital fingerprints**; these are typical program codes or certain access patterns which allow characterizing a certain group of attackers.[27]
These patterns can include the use of **malware families** (related sets of malicious codes), use of specific tools or tool combinations, scope of stealing, characteristic encryption algorithms, use of covert communication to control servers (such as mimicking legitimate communications) and language used (incl. typos, styles, preferred terms etc.) [28]. Also, information can be hidden into small pictures, a method known as **steganography**. Sometimes, attacker servers communicate with victim computers via Twitter or email.

Real world example: In early 2015, the security company *Kaspersky Labs* reported the existence of a new malware family called the *Equation group*. It is noteworthy that the malware could be tracked back to 2001, perhaps even to 1996. Due to technical overlaps, there are some things that may indicate that *Stuxnet* which was used against uranium centrifuges in Iran is part of a larger group of a malware family.[29] The Equation Group malware family included *EquationLaser*, *EquationDrug, Grayfish, Fanny, Double Fantasy* and *TripleFantasy***,** while the Stuxnet-related family included *Stuxnet, Flame, Duqu* and *Gauss* (with the derivates *MiniFlame* and *Duqu 2.0*[30]). Important links between the equation malware family and the Stuxnet-related malware family are the following[31]: In one infection step, *Grayfish* uses a hash code self-encryption step that shows similarities to the *Gauss* malware. *Fanny, Stuxnet, Flame* and *Gauss* use the same LNK exploit while *Fanny, Stuxnet, Double Fantasy* and *Flame* use a certain

[27] Mayer-Kuckuck/Koenen/Metzger 2012, p.20-21
[28] Mandiant 2013
29 Kaspersky Lab 2015a, p.3
[30] Kaspersky Lab 2015b, p.3
[31] Kaspersky Lab 2015a, p.5

escalation of a privilege account. Finally, *DoubleFantasy*, *Gauss* and *Flame* use a certain way of USB infection.

Meanwhile, the **programming styles** of certain programmers are also collected and analyzed, so that any new software programs can be compared with older ones ('stylometrics'). The NSA e.g. checks for way of setting brackets, use of variable names, empty spaces and programming text structure. Programming pieces are e.g. collected during hacking camps or by collection of informatics students works. However, a growing use of **obfuscation software** to replace names and modification of brackets is observed, too[32]. However, this does not allow clarifying whether an attacker worked on behalf of another state or authority.

Real world example: In 2016, a joint effort of IT security firms like *Symantec*, *Kaspersky, Alien Vault etc.* led by *Novetta* called *Operation Blockbuster* was made to analyze cases of cyber espionage and wiper attacks in Korea and US and the *Sony Pictures Entertainment (SPE)* hack 2014. The joint analysis showed strong evidence that at least two of the three large wiper attacks and the Sony/SPE hack were conducted by the same group called *Lazarus gr*oup. Novetta identified 45 malware families with multiple examples of **code re-usage** and **programming overlaps**. This included special issues like similar **Suicide Scripts** to remove executable malware programs after completion and a typical **space-dot-encoding**, where terms that could be detected by security software are spread by dots and normally unnecessary symbols between the letters. Also the programs included specific typos such a 'Mozillar' instead of ‚Mozilla' across several malware families and also there was a **reuse of a shared password** across malware droppers for different malware variants.

However, the *SPE hack* was one of the most controversial debates in the cyber attribution history, resulting from unexpected facts like the initial request for money, data distribution from outside of North Korea etc. etc[33][34]. Also, the mix of cyber espionage and suspect cyber criminal activities like the attack on the Interbanking system SWIFT was irritating[35].
However, most of the contradictions could be resolved, if the following assumptions are correct:
1. The SPE hack was initially a cyber-criminal activity which was escalated to political matter at a later stage. This would match the communication and attack pattern.

[32] Welchering 2016, p.T4
[33] Fuest 2014b, p.31
[34] The Security Ledger online 2014, p.1
[35] Brächer 2016, p. 26-27

2. The Lazarus group has a core of state-linked hackers which coordinate hackers in South East Asia. Thus would explain obscure findings like the long work times, the attack locations, overcome the issue of limited network capacities etc.

The SWIFT interbanking attack is of particular importance, because meanwhile it appeared that both the *Lazarus* group and *Carbanak*-related hacks **attacked independently the same target**. The wiping code used by the Lazarus group to hide the bank hacks *was the same* used in the SPE attack[36], while the latter used a new malware *Odinaff*[37].

Many people consider intrusion as a static event: once the malware is installed, the attacker can lean back and the data flow is going on. In reality, **cyber attack is a dynamic process**. The attacker may try to expand the access and control rights or push through to other computers of the intruded organization by **lateral movement**, i.e. from one system to the next. Updates have to be made and tailor-made modules are to be uploaded. Instructions have to be sent to the target computer.
Intruders have to pay attention that they are not discovered, e.g. by publication of an exploit they used. The extracted data have to be analyzed carefully to identify further needs or to realize when further attack is a waste of time and resources.
From this, it is difficult to mimic the attack of an APT even when the malware of the respective hacker group is available on the black market. The attacker needs to be aware that the cyber security companies do not present their full knowledge to the public, that the intelligence of member state may also know more about the usage and of course the original hacker group knows their malware better than others and not only *what* it used, but *how* and *when*.

Real world example: There were **overlaps between the attacks** of *APT28/Fancy Bears* on *French TV5 Monde*, the *German parliament Bundestag* and the *US Democratic National Convention DNC*. The attack on the *Bundestag* showed similarities to the cyber attack on TV5Monde[38]. One of the servers used for the Bundestag attack was identical with those used for the attack on the DNC in 2016 and also one falsified security certificate[39].

However, an attacker group could of course malware which is available on the black market, but even then they may show **core characteristics and programs** in use.

[36] Storm 2016
[37] Symantec 2016c
38 FAZ online 2015, see also Wehner 2015, p.1
39 Baumgärtner/Neef/Stark 2016, p.90-91

Real world example: The *Axiom group* was observed to do highly sophisticated spear-phishing attack by **piggybacking** (settling) on ongoing real conversations to motivate the victim to click on compromised links[40]. Note that the malware types *Zox* and *Hikit* were only seen in *Axiom* activities, while the other malware used by them was also used by other organizations[41].

Sophisticated hacker units can **check computers for pre-existing infections** (e.g. *Equation Group* and *Waterbug Group*) with their malware and if they detect infections of computers which were neither attacked nor infected earlier, they will be alerted. The hacker units may even be able to inspect the false flag attack and then the mimicking attacker has massive problems both in the digital and the physical world.

Real world example: The multi-functional malware named *Uroburos/Turla/Snake/Carbon* of the *Waterbug Group* is a rootkit that is able to connect computers within intranets as peer to peer-network and has multiple technical links to *agent.btz/Trojan Minit*[42] that caused the infiltration of Pentagon computers via USB sticks. Within this network, *Uroburos* is then searching for a computer that has internet access to conduct data exchange. It is noteworthy that *Uroburos* remains inactive in computers that are already infected by the malware indicating the same source[43].

In addition to the above analyses, the **chronology** of malware development is important to detect which malware could be derived from precursors and thus be related to the same attackers. For all sophisticated malware groups, such a chronology exists. Note that e.g. the *Stuxnet* malware not only had a long version history, but also massive changes of its structure and targets (originally valves, later centrifuges). [44]

Real world example: The new *APT Project Sauron* (also known as *Strider*) was discovered in 2016, but the malware properties indicate that the programmers have learned from other sophisticated malware, in particular *Duqu, Flame* (use of *Lua*

[40] Alperovitch 2014. The company *Crowd Strike* used a kernel sensor (*Falcon host*) deployed on Windows and Mac servers, desktops, and laptops that detected attacks and compared them to a threat intelligence repository for attribution.
[41] Novetta 2015, p.20. However, *Novetta* indicated in their *Winnti* attacker group analysis as part of the Operation SMN that *Hikit* was now used to leverage *Winnti* attacks. Whether this means that *Hikit* malware is now non-exclusive or *Winnti* (that changed from gaming industry to other industry espionage such as *ThyssenKrupp*) is now liaised with Axiom is not yet clear.
[42] Symantec 2016a, p.10-11
[43] Fuest 2014a, p.1-3
[44] McDonald et al. 2013, p.1-2

language), *Equation* and *Regin*, but at a time where these malware types were not discovered which may indicate a relation between the APTs[45].

Finally, a cyber crime attack does not end with computer communication, but the money gained by the attacks has to be transferred and hidden as well. This **whitewashing of money** is typically done with multiple transfers between banking accounts to obfuscate the origin of the money. The **use of digital bitcoins** does not really solve the issue, as at the end this has to be exchanged into real money again. The transfer of large sums of money and rapid moves are alert signals.
People who utilize their bank account for transfers of money are the so-called **money mules**, i.e. in addition to hackers further people are part of the cyber crime group. Experts identified the money transfer of cyber crimes as in important vulnerability of the attackers[46].

3.3Attack detection and prevention

Meanwhile attack detection can also be a real-time attribution.

Threat Intelligence repositories compare incoming information with known IP-addresses, domain names, websites and also with lists of known malicious attachments[47]. This allows immediate detection and sometimes even attribution of an incoming attack. Newly discovered malware can be integrated with so-called **Indicators of Compromise IOC**, i.e. numbers that allow detection in a certain computer.

In addition to standard recommendations on cyber defense such as strong passwords, updated systems, careful behavior in internet, avoiding suspect emails and attachments etc., an increasing effort is made on automated attack detection.

The US Government is currently expanding the use of advanced sensor systems[48]:
The **Continuous Diagnostics and Mitigation (CDM)** program provides real-time capacity to sense anomalous behavior and to create reports to administrators on a dashboard.
Einstein 3A is working by installing sensors at Web access points to keep threats out while CDM should identify them when they are inside.

For cyber defense, US researchers have developed **pattern recognition algorithms**, which allow after attack detection the automated deletion of data

[45] Kaspersky 2016, p.21, Symantec 2016
[46] Baches 2016, p.15
[47] The company *Crowd Strike* uses a kernel sensor (*Falcon host*) deployed on Windows and Mac servers, desktops, and laptops that detect attacks and compare them with a threat intelligence repository for attribution.
[48] Gerstein 2015, p.4-5

packages that are part of the cyber attack. To avoid escalation, retaliation to networks or systems is not automated. China is researching on attack simulation[49].

The German *Deutsche Telekom* has installed 200 **honey pot** computers that simulate average mobile phones and computers. The honey pot computers are able to document each step of the intruder[50], the analysis environment is also known as **sandbox**. As advanced malware stays silent in virtual machines, advanced sandboxes try to mimic real computers as far as possible. On the other hand, malware may be protected by **code morphing**, an approach used in obfuscating software to protect software applications from reverse engineering, analysis, modifications, and cracking.

An important progress is the formation of **Cyber alliances**, e.g. the *Cyber Threat Alliance* of the security firms *Fortinet, Intel Security, Palo Alto Networks* and *Symantec* to fight against ransomware. More and more private security firms merge collected data and do-long-term analyses to identify certain groups. Examples are the large forensic Operations *SMN* and *Blockbuster*, more details will follow below. As sophisticated attacks are typically executed by groups that operate over years and not as isolated 'hit and run'-incidents, attribution efforts are increasingly effective. Also, large private companies coordinate their cyber defense, e.g. in the *Deutsche Cyber Sicherheitsorganisation DCSO (German Cyber Security Organization)* with *VW*, *BASF*, *Allianz and Bayer*.

3.4 Human Intelligence

The identification of an attacker is sometimes out of reach for digital attribution methods. Human intelligence methods can help to find the missing link.

The following methods are most important in the practice of attribution:

- Cyber intelligence
- Intelligence cooperation for information exchange
- Conventional intelligence.

3.4.1 Cyber intelligence

As a general outline, it is known that many companies including IT security companies provide information on potential exploits to the intelligence *before* the exploits are published or closed by patches to support intelligence activities[51]. As a practical consequence, user of devices, software or IT security software have to

[49] Welchering 2014b, p.T4
[50] Dohmen 2015, p.75
[51] FAZ 2013, p.1

consider the possibility that the intelligence of the manufacturer/provider country *may* have and use access, that by intelligence cooperation an indirect access *may* also exist for further agencies from other countries and that a zero day-exploit *may* not be 'zero' at all. Together with the surveillance of information flow[52] and the above described intelligence access to encryption systems, cyber security *between* computers may also be a problem. The decision on keeping exploits secret is based on a thorough risk-benefit assessment, i.e. who else could use it, how large is the risk of disclosure and damage to own users and companies[53].

In military sector, *preparing the battlefield* is essential for successful strategies, in practice this means to place **beacons** or **implants** into foreign computer networks, this is code to monitor how these networks work[54].

Another issue is **pre-encryption access**, as providers often decrypt data for internal handling and re-crypt afterwards. By accessing node servers, intruders can bypass encryption.

Real world example: some countries asked the Blackberry provider *Research in Motion (RIM)* in 2010 to put servers into their own countries[55]. However, meanwhile many providers are confronted with requests to put servers into a country by many countries all over the globe, this is meanwhile a normality which makes control of data flow and attribution much easier. This again underlines the importance of physical elements in the digital world.

Another targeted approach is the collection and analysis of **user profiles**. In March 2012, *Google* announced that profiles of users can be compiled by combining data from search engine usage, *YouTube, Google plus* and *gmail*[56]. Similar procedures are also known from social network companies, but *Google* and other companies were affected in 2013 by a presumably Chinese hacking by which profiles of Chinese users were checked and exported[57].

Hack the hackers: If the attackers are identified, it may make sense to intrude them to find out more about their activities.

---

[52] This includes conventional surveillance of paper-based and analog communication as well as interception of information from optical fibers, Gutscher 2013b, p.7, Welchering 2013b, p.6. Also, in line with respective national law, e.g. the 1994 **Communications Assistance for Law Enforcement Act (CALEA)** and the **Foreign Intelligence Surveillance Act (FISA)** in US, providers may give technical access to data or systems.
[53] Daniel cited in Abendzeitung 2014
[54] Sanger 2015, p.5
[55] Schlüter/Laube 2010, p.8
[56] Spiegel 2013, p.111
[57] Süddeutsche Online 2013

Real world example: the *New York Times* reported that the NSA would have been able to intrude North Korean network via Malaysia and South Korea which enabled them to observe and track North Korean hacking activities, but this report was not officially confirmed[58].

In 2017, the Cyber security company *Cellebrite* was hacked and data were published. These showed that 40,000 licensed clients (intelligence, border police, police, military units, finance organizations) used e.g. the *Universal Forensic Extraction Device UFED* that allows access to smartphones by utilizing security gaps (exploits). Further exploit collections for *iOS, Android* and *Blackberry* were released[59].

3.4.2 Intelligence Cooperation

Media reports in 2013 gave the impression, that Intelligence cooperation is focused on computers and Signals Intelligence SigInt. However, intelligence cooperation was created during World War II, and was expanded during Cold War and in response to growing terrorist activities already in the decades before 9/11. As a result, the intelligence cooperation also includes the collection and analysis of information derived from human intelligence (HumInt), imaging intelligence (ImInt) and open source intelligence (OsInt)[60].

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. The standard solution is to have multiple organizations with a coordinating level[61]. 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*[62].

The second level is a network of **bilateral intelligence cooperation**, e.g. Germany has relations with more than 100 countries[63]. 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

58 FAZ 2015, p.5.
59 Kurz 2017, p.13
60 Best 2009
61 Carmody 2005
62 DNI Handbook 2006
63 Daun 2009, p.72

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. Smaller groups can easier have deep 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[64].

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)*[65] is analyzing information provided by member state organizations, counter-terrorist working groups etc. [66] Africa has established the multinational cooperation *Committee of Intelligence and Security Services of Africa CISSA* a part of the African Union.

3.4.3 Conventional intelligence

Recent events from 2016 illustrate the relevance of conventional intelligence activities for attribution. As shown above, the tensions between Russia and US were already ongoing, as the Russian security firm *Kaspersky* used sinkholing against the presumably US-based *Equation Group*[67], while they on the other hand infected *Kaspersky* with the sophisticated espionage malware *Duqu 2.0* [68].

In August 2016, a previously unknown group called *Shadow Brokers* claimed to have cyber weapons from the *Equation Group* (which is suspected to have relations to US) and published material. Media speculated that this was a symbolic warning by Russia that was accused for the **DNC hack** by media, i.e. to show that they are also able to trace and unveil espionage from others as needed[69]. The analysis of the public file showed that it was software from 2013, the assumption

[64] See e.g. Shane 2013, p.4
[65] Note of 22 October 2009 which was followed by a Draft Council Decision: Council Decision on setting up the Standing Committee on operational cooperation on internal security (EU doc no: 16515-09 and EU doc no: 5949-10).
[66] Scheren 2009
[67] Kaspersky Lab 2015a, p.34-35
[68] Kaspersky Lab 2015b
[69] Jones 2016

of security experts was that this material was copied from a command and control server used by the *Equation Grou*p, i.e. no 'NSA hack' or similar.
Later on the *Shadow Brokers* also released a list of IP addresses of computers which were infected and used by *Equation Group*.
In a later statement on *Pastebin* and *Tumblr* –claimed to come from the hackers- they explained that a contractor from the company *RedSeal* took away copies after a security exercise[70]. The material seemed to be real and some file names were identical to names presented by *Edward Snowden* as NSA tools, such as *Epicbanana, Buzzdirection, Egregiousblunder, Bananaglee, Jetplow and Extrabacon*[71].
In the USA, 1.5 million people in US have a cyber-relevant security clearance level, thereof 480,000 from private companies[72]. Moreover, the ODNI was cited that 70% of the intelligence budget is assigned to private firms[73]. On the other hand, it was argued that the cooperation with private firms is already long-standing[74] and would be necessary to utilize expert knowledge in the rapidly growing cyber sector.

The **Michailow incident:** End of August 2016, it was detected that online voting systems were intruded in Illinois and Arizona, in Illinois data of 200,000 voters were copied[75]. Media speculated that this was part of a Russian campaign, but definite evidence was not found.[76] But then it was detected that a company named *King Server* leased six servers for this attack from a company called *Chronopay*. The Russian owner of *Chronopay* was already under investigation by *Sergej Michailow*, a member of the Russian Intelligence Cyber Unit CIB of the intelligence service FSB who (according to reports e.g. from the newspaper *Kommersant*) informed US authorities about this matter[77]. *Russia Today* confirmed that there are issues with Mr. Michailow without confirming the details of the information leak, but clarified that the case together with others is still under investigation by Russian authorities[78].

The **Surkov incident:** In mid of October 2016, US Vice President *Joe Biden* announced that US seriously considers a cyber retaliation against Russia due to their suspected involvement in the *DNC hack* and other issues[79]. A few days later,

[70] Ragan 2016
[71] Steier 2016, Spiegel online 2016, Solon 2016
[72] Gartmann/Jahn 2013, p.24
[73] Huber 2013, p.18-19
[74] BAH cracked German submarine codes in WWII, Gartmann/Jahn 2013, p.24. Other security firms are e.g. Xe and USIS.
[75] Nakashima 2016, Winkler 2016, p.4
[76] Winkler 2016, p.4
[77] FAZ 2017, p.5
[78] Russia Today (RT Deutsch) online 27 Jan 2017
[79] Zeit online 2016

i.e. before the Presidential Elections in US, a Ukrainian Group named *CyberHunta* presented the hack of the email box of the Bureau of the Russian President's top advisor *Vladislav Surkov*. At least parts of the material could be verified as real, i.e. as not fabricated. However, US media doubted that such a top-level operation could be done by a Ukrainian Group without respective hacking history, but that this was instead a warning by US intelligence[80].

The *US Intelligence Community Report* on Cyber incident Attribution from 2017 which was in line with the preceding assessment on the operations of *APT28/Fancy Bears* and *APT29/Cozy Bears* as Operation *Grizzly Steppe* strongly emphasized the political motivation of Russia as argument for the attribution of the attacks to Russia[81]. This was criticized in media as limited evidence, but the *Michailow* and *Surkov incidents* indicate that there was possibly more behind the scene than only digital attribution and analysis of political motivations.

4. Attribution in Cyber War

The term **Cyber war** (also cyberwar, cyber warfare, computer warfare, computer network warfare) is a combination of the terms war and cyberspace and designates the military conflict with the means of the information technology.
The attribution in cyber war is from the theoretical and legal perspective the most important attribution problem as the question "who did it?" may result in retaliation or even war if a certain level of damage is exceeded.
However, the practical relevance of the matter is unclear as there is an **attribution paradox**.

First, the cyber war concepts of US and China agreed from the very beginning that the use of computers in military activities is only part of other military activities. The debate on the question whether a war can be decided by computer attacks alone is only a theoretical one, for the military practice this option was never taken into consideration.

[80] Shuster 2016

[81] ODNI 2017, JAR 2016 of the Department of Homeland Security DHS and the Federal Bureau of Investigation FBI. *APT 28/Fancy Bears* and *APT29/Cozy Bears* are groups focusing on targets of political relevance for Russia. The malware compilation times correspond with Moscow time zone, Russian language is used, and typically tools for continued long-term use are used. *APT 28* backdoors use http protocol and the mail server of the target computer, see Weedon 2015. *APT 28* uses a variety of malware droppers (*Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer and DownRange*) and also malware for smartphones, see Alperovitch 2016. *The Dukes* are a malware family with a growing number of toolsets known as *MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke* and *GeminiDuke* which are used by *APT29/Cozy Bears*, see Weedon 2015. The attacks show a two-step pattern with initial breach and rapid data collection, then in case of a relevant target changing to long-term observation tools, see F-Secure Labs 2015. For this action, multi-step loading and backdoors are available. To avoid detection, the malware checks the security measures of the infected computer in detail.

Sometimes it is further debated whether computers could really be a part of a war as computer attacks could not kill people, but in military practice this debate is misleading. Computers are simply technical tools as e.g. *Radar systems*. Radar systems do not kill enemies directly and indeed, they save a lot of lives in civil air traffic, but nobody would doubt that Radar systems are part of military activities as well.

General *Keith Alexander,* the previous commander of the US Cyber Command CYBERCOM and the NSA, outlined his perspective on cyber warfare already in 2007 and described it as an integral and *supportive* activity and not a stand-alone military concept. Also, the concept includes defensive and not only offensive components[82]. As a consequence, cyber war is done as common action of humans and computers and is usually a group of activities and not only a single hit even if a surprising action may start the war. The primary aim of actors is to achieve and maintain **electromagnetic dominance** and **cyberspace superiority**[83] in particular, that is to control the cyberspace during a conflict. As the system of the adversary can be restored after some time, the practical goal is to achieve the **freedom of action** for the own forces and to limit the others at the same time. The cyber activities are combined with conventional operations.

The Chinese cyber strategy is to hit the enemy network first and to check the resulting ‚**operational blindness**' with conventional weapons and to continue attack, if possible[84]. Of course, the enemy may be able to repair the network and the strategy may not be successful, thus it is necessary to get electromagnetic dominance as early as possible and to maintain this as long as possible. Also the enemy may not be hit as expected and is still able to react. US studies indicated that such a war can only be conducted for a limited time.[85]

The US and Chinese cyberwar concepts clearly indicate that a conventional strike must be executed simultaneously or very shortly after the cyber attack if the military action should be successful. This means that the attribution of the cyber attack will be possible within minutes, because the target state will at the same time exposed to hostile fire, i.e. the attacker will identify himself.

Real world example: On 06 September 2007, a suspected nuclear plant in Eastern Syria was destroyed by Israeli air attacks. Israel was technically able to simulate a free heaven to Syrian air defense systems and could thus conduct this attack without disturbance[86].

[82] Alexander 2007, p.60
[83] USAF 2010, p.2
[84] Krekel et al. 2009
[85] Tinnel et al. 2002
[86] Herwig 2010, p.60

If a massive cyber attack would be done without an accompanying conventional strike, the target state has time to restore the systems first and to start attribution in the meantime as well, which with aggressive use of intelligence methods may take less time than attackers expect.
On the other hand, this results in a kind of **reverse attribution**, i.e. from the physical to the digital world. In the era of espionage satellites, the preparation of a large military strike will not be undetected and is typically coming after massive political tensions, i.e. there are clear warning signs in the physical world for coming attacks in the digital world.

5. Concluding Remarks

The paper has shown that attribution is a cyber-physical process that includes the digital and the physical world.
Attribution efforts have made substantial progress in the last years and further rapid progress can be expected. However, the attackers will probably ever one step ahead, because hackers will continue to find new vulnerabilities and previously unexpected ways to attack computers and devices.
Attribution is not only about gathering information, the interpretation and combination of facts is also important. The attribution discussion is often controversial and thus, any deviating theory needs to be checked whether it presents new facts or better interpretations of the existing findings.
The cooperation between organizations by combination of resources, experience and knowledge will be a key element for future success in attribution of cyber attacks.

6. Literature References

Abendzeitung (2014): USA halten einige Lücken in Computersystemen geheim. Abendzeitung online 29 Apr 2014

Alexander, K.B. (2007): Warfighting in Cyberspace. JFQ, issue 46, 3rd quarter 2007, p.58-61

Alperovitch, D. (2014): Deep in Thought: Chinese Targeting of National Security Think Tanks 07 Jul 2014, 8 pages

Alperovitch, D. (2016): Bears in the Midst: Intrusion into the Democratic National Committee. From The Front Line, update 15 Jun 2016, 3 pages

Alvarez, S., Jansen, F. (2016): Hackerangriff auf die Telekom. Der Tagesspiegel online 28 Nov 2016

Baches, Z. (2016): Wie Hacker eine Notenbank knacken. Neue Zürcher Zeitung, 10 Oct 2016, p.7

Baumgärtner, M., Neef, C. Stark, H. (2016): Angriff der Bären. Der Spiegel 31/2016, p.90-91

Best, R.A. (2009): Intelligence Issues for Congress. CRS Report RL33539

Brown, G., Poellet, K. (2012): The Customary International Law of Cyberspace. In: Strategic Studies Quarterly. Volume 6 Fall 2012 Number 3, p.126 ff.

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

Brächer, M. (2016): Das fragile Netzwerk. Handelsblatt No. 155/2016, p.26-27

Chiesa, R. (2015): Lectio Magistralis Hacking Cybercrime e underground economy (con u po di cyber espionage) Arcetiri, Firenze, INFN 5 Novembre 2015

Daun, A. (2009): Die deutschen Nachrichtendienste. In: Geheimdienste in Europa. Transformation, Kooperation und Kontrolle VS Verlag für Sozialwissenschaften, p.56-77

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

Dohmen, F. (2015): Überfall in 5 Minuten, Der Spiegel 20/2015, p.74-75

EUROPOL (2016): 'Avalanche' Network dismantled in International Cyber Operation. Press Release 01 December 2016

EU (2016): Commission Services Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace. Brussels, 2 December 2016 15072/16

FAZ (2013): Tausende Unternehmen informieren Geheimdienste. Frankfurter Allgemeine Zeitung No. 136, 15 Jun 2013, p.1

FAZ (2015): “NSA hat Computer in Nord Korea schon vor 4 Jahren infiltriert”. Frankfurter Allgemeine Zeitung, 20 Jan 2015, p.5

FAZ online (2015): Cyber-Angriff auf TV5 Monde. Ermittler verfolgen Spur nach Russland. FAZ online 09 Jun 2015

FAZ (2017): Geheimdienstler verhaftet. Frankfurter Allgemeine Zeitung, 28 Jan 2017, p.5

FireEye (2014): APT28: A Window into Russia’s Cyber Espionage Operations? 45 pages

Fuest, B. (2014a): Uroburos –Russisches Supervirus greift die Welt an. Welt am Sonntag online 10 March 2014, 3 pages

Fuest, B. (2014b): Der übliche Verdächtige. Welt Am Sonntag No.52/2014

Gartmann, F., Jahn, T. (2013): Die Geheim-Dienstleister. Handelsblatt 26 Jun 2013, p.24

Gerstein, DM (2015): Strategies for Defending U.S. Government Networks in Cyberspace. RAND Office of External Affairs Document CT-436 June 2015, 7 pages

Glenny, M. (2010): Die neuen Cyberkrieger. Financial Times Deutschland, 12Oct 2010, p.23/26

Guerrero-Saade, J.A., Raiu, C. (2016): Operation Blockbuster revealed. Securelist. https://securelist.com/blog/incidents/73914, 10 pages

Gutscher, Th. (2013b): Menschenrechte hochhalten, nach Daten tauchen. Frankfurter Allgemeine Sonntagszeitung No.26 30 Jun 2013, p.7

Herwig, M. (2010): Die @-Bombe. Welt Am Sonntag No.39, 29 Jun 2010. p.60-61

Huber, M. (2013): Der entkernte Staat. Der Spiegel 25/2013, p.18-19.

JAR (2016): Grizzly Steppe –Russian Malicious Cyber Activity. JAR-16-20296, December 29, 2016, 13 pages

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

Johnson, A. et al. (2013): Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries. US Naval Research Laboratory.

Jones, S. (2016): Cyber espionage: A new cold war? 19 Aug 2016 Financial Times online, 7 pages

Kaspersky (2013): “Winnti” Just more than a game. April 2013, 80 pages plus appendix

Kaspersky (2014): Unveiling Careto – The masked APT February 2014

Kaspersky Lab (2015a): Equation Group Questions and Answers. Version 1.5, February 2015, 32 pages

Kaspersky Lab (2015b): The Duqu 2.0 Technical details. Version 2.0, 9 June 2015, 45 pages

Kaspersky Lab (2015c): Der große Bankraub: Cybergang “Carbanak” stiehlt eine Milliarde US-Dollar von 100 Finanzinstituten weltweit, Moskau/Ingolstadt, 15 February 2015, 3 pages

Kaspersky (2016): The Project Sauron APT August 2016, 14 pages

Kramer, A. (2016): How Russia Recruited Elite Hackers for Cyberwar. New York Times 29 Dec 2016

KrebsonSecurity (2016): Carbanak Gang Tied to Russian Security Firm? Official Security Blog of Brian Krebs 2016

KrebsonSecurity (2017): Who is Anna Sempai, the Mirai Worm author? Official Security Blog of Brian Krebs 20 Jan 2017

Krekel, B. (2009): Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network. Exploitation Prepared for The US-China Economic and Security Review Commission. Northrop Grumman Corporation. October 9, 2009

Kurz, C. (2017): Jetzt ist es an der Zeit, die Lücken zu schließen. Frankfurter Allgemeine Zeitung No. 31, 06 Feb 2017, p.13

Mandiant (2013): APT 1 Exposing One of Chinas Cyber Espionage Units, 74 pages

Mayer-Kuckuck, F., Koenen, J., Metzger, S. (2012): Hacker werden immer dreister. Handelsblatt 15 Feb 2012, p.20-21

McDonald, G., O’Morchu, L., Doherty, S., Chien, E. (2013): Stuxnet 0.5: The Missing Link. Symantec Report 2013, 18 pages

Müller, G.V. (2016): Der Verpächter des Internets. Neue Zürcher Zeitung, 01 Nov 2016, p.7

Nakashima, E. (2016): Russian hackers targeted Arizona election system. Washington Post online, 29 Aug 2016, 4 pages

Novetta (2015): Operation-SMN-Report June 2015, 31 pages

Novetta (2016): Operation-Blockbuster-Report February 2016, 59 pages

ODNI (2017): Intelligence Community Assessement Assessing Russian Activities in Recent US Elections, 14 pages

RadioFreeEurope (2016): ---hacking Group from Russia, China Claims Credit for a Massive Cyberattack. 13 Oct 2016

Ragan, S. (2016): Salted Hash – Top Security News. Hackers say leaked NSA tools came from a contractor at Red Seal. CSO online article 3109936, 6 pages

Raiu, C., Baumgartner, K., Kamluk, V. (2013): The MiniDuke Mystery. PDF 0-day Government Spy Assembler 0x29A MicroBackdoor, 20 pages

Rosenbach, M. (2016): Hacker aus dem Staatsdienst. Der Spiegel 40/2016, p.78-79

Russia Today (RT Deutsch) online (2017): Russland: FSB und Kaspersky Lab in Erklärungsnot – Landesverrat im Bereich Cybersicherheit vermutet. 27 Jan 2017

Sanger, D.E. (2015): US and China seek arms deal for cyberspace. New York Times online 20 Sep 2015, 5 pages

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.

Schlüter, N., Laube, H. (2010): Der RIM-Code. Financial Times Deutschland 03 Aug 2010, p.8

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

Shuster, S. (2016): Hacker Kremlin Emails could signal a turn in the U.S.-Russia Cyberwar. Time Magazine online 07 Nov 2016

Solon, O. (2016): Hacking group auctions 'cyber weapons' stolen from NSA. The Guardian online, 16 Aug 2016, 2 pages

Spiegel (2013): Verdacht statt Vertrauen, Der Spiegel 26/2013, p.111

Spiegel online (2016): Gruppe "Shadow Brokers" Hacker erbeuteten offenbar NSA-Software. 17 Aug 2016, 1 page

Steier, H. (2016): Riskantes Horten von Sicherheitslücken. Neue Zürcher Zeitung online, 18 Aug 2016, 2 pages

Storn, A. (2016): Plötzlich sind 81 Millionen Dollar weg, Die Zeit No.20, 04 May 2016, p.29

Symantec (2014a): Regin: Top-tier espionage tool enables stealthy surveillance. Symantec Security Response Version 1.0 – November 24, 2014, 22 pages

Symantec (2016a): The Waterbug attack group. Security Response Version 1.02 Symantec, 14 Jan 2016, 44 pages

Symantec (2016b): Strider: Cyberespionage group turns eye of Sauron on targets, Symantec Official Blog, 07 Aug 2016

Symantec (2016c): Odinaff: New Trojan used in high level financial attacks, Symantec Official Blog, 11 Oct 2016

SZ online (2013): Fernseher schaut zurück. Report on 21 Nov 2013

Tellenbach, B. (2017): Darknet macht keinen neuen Kriminellen. Neue Zürcher Zeitung 17 Feb 2017, p.31

The SecurityLedger online (2014): New Clues in Sony Hack point to insiders, away from DPRK, page 1 18 Dec 2014

Tinnel, L.S., Saydjari O.S., Farrell D. (2002): Cyberwar Strategy and Tactics. An Analysis of Cyber Goals, Strategies, Tactics, and Techniques. Proceedings of the 2002 IEEE Workshop on Information Assurance. United States Military Academy, West Point, NY June 2002, p.228-233

USAF (2010): US Air Force Doctrine Document (AFDD) 3-12, Cyberspace Operations 15 July 2010, 55 pages

Weedon, J. (2015): Beyond ‚Cyber War': Russia's use of strategic espionage and information operations in Ukraine. In: Geers, K. Cyberwar in Perspective Russian aggression against Ukraine. NATO CCD COE Publications. Tallinn 2015, p.67-77

Wehner, M. (2015): Cyber-Krieg im Bundestag. Frankfurter Allgemeine SonntagsZeitung. Nr.24 from 14 June 2015, p.1

Welchering, P. (2013): Mit Vierkantschlüssel und Biege-Koppler. Frankfurter Allgemeine Zeitung No. 156/2013, p.6

Welchering, P. (2014): Arbeiten am Trojaner-Abwehrschirm. Frankfurter Allgemeine Zeitung from 09 September 2014, p.T4

Welchering, P. (2016): So fahndet der Geheimdienst NSA nach Programmierern. Frankfurter Allgemeine Zeitung No. 136/2016, p.T4

Winkler, P. (2016): Russische Hacker in Amerikas Wahlregistern. Neue Zürcher Zeitung, 01 Sep 2016, p.4

Wittmann, J. (2017): Gesucht: Bond. Jane Bond. Neue Westfälische 11 Feb 2017

Zeit online (2016): Mögliche CyberAttacke soll Russland bloßstellen. October 2016, 2 pages

Zepelin, J. (2012): Länder lahmlegen. Financial Times Deutschland 06 Jul 2012, p.27