UNIVERSITÄT OSNABRÜCK

LV Internet policy
Fachbereich 1
49069 Osnabrueck

Attribution von Cyber-Attacken

Methoden und Praxis

Arbeitspapier – 17.02.2017

Zusammenfassung

Attribution bezeichnet die Zuordnung einer Cyberattacke zu einem bestimmten Angreifer bzw. Angreifergruppe im ersten Schritt und die Aufdeckung der tatsächlichen Identität des Angreifers in einem zweiten Schritt. Während sich die Methodik der Zuordnung einer Cyberattacke zu bestimmten Angreifern in den letzten Jahren deutlich weiterentwickelt hat, erlauben Digitaltechnologien oft nicht den eindeutigen Nachweis der tatsächlichen Identität des Angreifers.
Die Situation sieht anders aus, wenn die Attribution als *cyber-physischer Prozess* gehandhabt wird, d.h. als Kombination aus digitaler Forensik und Beweisführung in der physischen Welt.
Bits und Bytes sind nämlich nicht wirklich virtuell, sondern nach wie vor an eine physische Infrastruktur in der realen Welt gebunden, was verschiedene Möglichkeiten zur Erkennung von Gegnern bietet. Lücken in der Beweisführung können auch mit Mitteln der Human Intelligence (HumInt) geschlossen werden.
Dieses Papier gibt einen Überblick über die aktuellen Methoden der Attribution mit realen Praxisbeispielen.

Inhalt

1. Grundlagen

1.1 Einführung

Attribution bezeichnet die Zuordnung einer Cyberattacke zu einem bestimmten Angreifer bzw. Angreifergruppe im ersten Schritt und die Aufdeckung der tatsächlichen Identität des Angreifers in einem zweiten Schritt. Während sich die Methodik der Zuordnung einer Cyberattacke zu bestimmten Angreifern in den letzten Jahren deutlich weiterentwickelt hat, erlauben Digitaltechnologien oft nicht den eindeutigen Nachweis der tatsächlichen Identität des Angreifers.

Die Situation sieht anders aus, wenn die **Attribution als cyber-physischer Prozess** gehandhabt wird, d.h. als Kombination aus digitaler Forensik und Beweisführung in der physischen Welt.

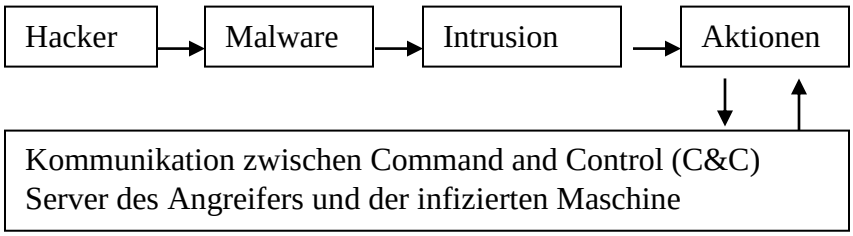
Bits und Bytes sind nämlich nicht wirklich virtuell, sondern nach wie vor an eine physische Infrastruktur in der realen Welt gebunden, was verschiedene Möglichkeiten zur Erkennung von Gegnern bietet. Lücken in der Beweisführung können auch mit Mitteln der Human Intelligence (HumInt) geschlossen werden.

Dieses Papier gibt einen Überblick über die aktuellen Methoden der Attribution mit realen Praxisbeispielen.[1].

1.2 Hintergrund

1.2.1 Die Grundlagen einer Cyberattacke

Cyber-Angriffe erfordern das Eindringen (**Intrusion**) in das digitale Gerät, d.h. den Computer, Smartphone oder andere Arten von digitalen Geräten mit einem Schadprogramm (Malware) und die Kommunikation mit den intrudierten Geräten, um Aktionen zu starten. Abhängig von der Art der Aktion wird die Kommunikation für eine längere Zeit aufrechterhalten, mitunter auch über Jahre; komplexe Angriffe erfordern in der Regel eine *bidirektionale* Kommunikation, die vielfältige Möglichkeiten zur Erkennung und Zuordnung bietet.



[1] Dieses Arbeitspapier konzentriert sich ganz auf die Attribution. Für Hintergrundinformation mit Blick auf Eindringmethoden, Terminologie, rechtliche, politische und organisatorische Aspekte wie auch zur Geschichte von Hackergruppen wird auf das frei zugängliche Papier "Cyberwar-Grundlagen-Methoden-Beispiele" http://www.dirk-koentopp.com/downloads/saalbach-cyberwar-grundlagen-geschichte-methoden.pdf, und die dort zitierte Literatur verwiesen.

Derzeit sind die häufigsten und herausragenden Cyber-Attacken:

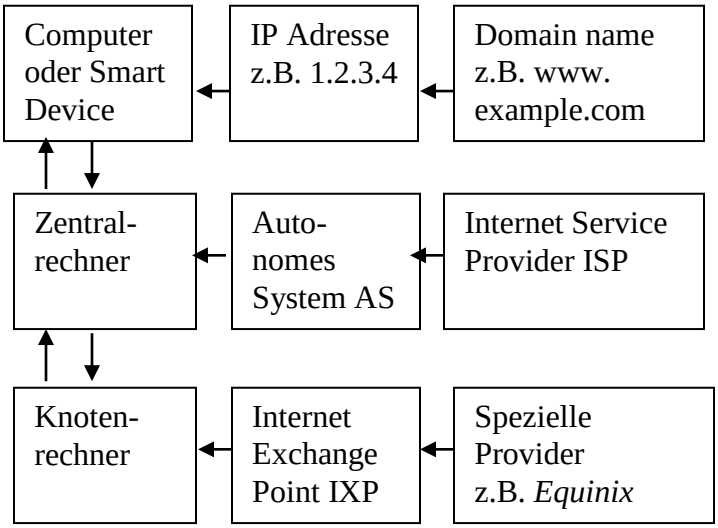
- Malware-Installation für alle Arten von Cyber-Spionage (Militär, Politik, Industrie, Finanzsektor, Forscher, internationale Organisationen etc.). Manchmal ist dies mit der Verwendung von Cyber-Waffen wie **logischen Bomben** und **Wiper-Malware** kombiniert
- Errichtung von Botnetzen, d.h. Gruppen von infizierten und kontrollierten Maschinen, die missbraucht werden, um automatisierte und sinnlose Anfragen an einen Zielcomputer oder -system zu senden, das dann zusammenbricht (verteilte = distributed Denial-of-Service-Angriffe, kurz **DDoS-Angriffe**). Dies kann aus politischen Gründen geschehen, aber auch, um das Opfer im Rahmen der Cyberkriminalität zu erpressen
- Die Installation von Crimeware wie **Ransomware**, die das Gerät verschlüsselt, woraufhin vom Opfer Geld für den Entschlüsselungscode verlangt wird, und Banking-Trojaner, um Zugang zu Online-Banking-Konten zu erhalten.

1.2.2 Kommunikationswege der Cyberattacken

Daten, d.h. Bits und Bytes sind nicht vollständig virtuell, sondern sind immer noch physikalisch als definierter elektromagnetischer Zustand auf Speichermedien und Gerätespeichersystemen vorhanden[2]. Die drahtlose Übertragung führt zu elektromagnetischen Wellen und schließlich enden diese Wellen am Ende wieder physisch in Geräten. Dieser Befund ist für die Erkennung und Zuordnung essentiell. Da die Kommunikation über Computer-Netzwerke erfolgt, ist es hilfreich, die allgemeine Infrastruktur des Internets im Auge zu behalten: Diese Struktur bildet auch das ‘digitale Ökosystem’ der Hacker, das im nächsten Abschnitt 1.2.3 dargestellt wird.

[2] Dies mag trivial erscheinen, aber bedeutet das gelöschte Daten auf einem Gerät **nicht ausradiert** sind. Das Gerät markiert die Datei nur als ‘gelöscht’ und sie erscheint nicht mehr auf dem Bildschirm. In Wirklichkeit befinden sich die Daten weiterhin auf dem Speichermedium, so dass “gelöschte” Daten mit Hilfe forensicher und Spionage-Techniken wiederhergestelt werden können.

Vereinfachtes Modell der Internetkommunikation



Typischerweise startet eine Internetkommunikation bei einem bestimmten Computer und die Daten werden dann an den zentralen Rechner eines **Internet Service Providers (ISP)** übertragen. Dieser zentrale Computer wird offiziell als **Autonomes System (AS)** bezeichnet und große Anbieter können viele davon haben. Allerdings müssen die Internet Service Provider miteinander verbunden sein, dies geschieht über Knotencomputer, die offiziell als **Internet Exchange Point (IXP)** bezeichnet werden. In Wirklichkeit sind dies große Rechenzentren und nicht nur einzelne Computer.

Jeder Computer, der mit dem Internet verbunden ist, hat eine **IP-Adresse (IP = Internetprotokoll)**, eine nach bestimmten Regeln strukturierte Zahl. Das alte 4-stellige System der IP-Version 4 wird nun durch größere Bausteine der IP-Version 6 ersetzt, aber das Prinzip, dass eine Domain mit einer IP-Adressnummer zu einem bestimmten Zeitpunkt verknüpft ist, bleibt gleich. Dies hat die gleiche Funktion wie Telefonnummern für Telefone, d.h. die technische Möglichkeit, Sender und Ziel richtig zu verbinden.
Webseiten haben auch IP-Adressen, aber stattdessen werden normalerweise **Domain-Namen** verwendet, z.B. www.example.com. Zu einem definierten Zeitpunkt beziehen sich Domainnamen jeweils auf bestimmte IP-Adressen, um Kommunikationsverwechslungen zu vermeiden.

Infolgedessen mag das Internet im Alltag dezentral und virtuell erscheinen und es scheint fast sinnlos, herauszufinden, woher ein Cyberangriff kam.
In der physischen Welt ist das Internet jedoch am Ende an ein physisches Netzwerk mit einer signifikanten Zentralisierung gebunden. Das US-amerikanische Unternehmen *Equinix* steuert mit eigenen IXPs und Co-Location

von Client-Computern in ihren Rechenzentren rund 90% (!) der Datenübertragung des Internets[3]. Wie im folgenden gezeigt wird, bietet dies Möglichkeiten, Einblick in die Infrastruktur des Gegners zu bekommen.

1.2.3 Ein erster Schritt zur Attribution

Theoretisch kann ein Hacker einen einzigen Angriff von "irgendwo" starten und es mag unmöglich sein, diesen zurück zu verfolgen. Auf der anderen Seite ist die Erfolgsquote dieses Ansatzes recht niedrig.
Angreifer, die einen bedeutenden Erfolg erzielen wollen, greifen typischerweise in einem größeren Maßstab an, d.h. als Gruppen, mit anspruchsvoller Malware und agieren manchmal über Jahre. Je länger und je intensiver der Angriff ist, desto höher ist das Risiko für Erkennung und Attribution.

Der Datenverkehr des Computers erfolgt über sogenannte **Ports**. Ein Supervisor (IT-Administrator) kann die Ports und den Datenverkehr mit handelsüblichen Tools überprüfen. Diese Tools zeigen auch, an welche IP-Adresse die Daten gehen oder gegangen sind.
Nun gibt es spezialisierte Suchmaschinen, die automatisch überprüfen, was hinter einer IP-Adresse steht. Ein Beispiel für solche Maschinen ist *Robtex.com*. Die Anbieter dieses Dienstes erklären auf ihrer Website, dass dieses Tool "nicht nur" von der *National Security Agency NSA* verwendet wird, was darauf hinweist, dass diese Dienste auch als Intelligence-Tools dienen.

Durch die Eingabe der IP-Adresse in die Suchmaske zeigt *Robtex* Datenströme mit anderen IP-Adressen sowie den Weg zum autonomen System AS oder dem Internet Service Provider ISP. *Robtex* kombiniert IP-Adressen und Domains sowie alle existierenden Subdomains. Außerdem zeigt es die Mail-Server im Zusammenhang mit dem Domain-Namen.

Dies ist aus folgenden Gründen wichtig:

- Angreifer behalten oft eine gewisse Angriffsstruktur bei, denn wie jedes Konstrukt hat eine Angriffsumgebung sowohl Bau- als auch Ausstiegskosten. Infolgedessen werden Mailadressen, Domainnamen, Server und IP-Adressen zumindest teilweise von einem Angriff zum nächsten recycelt. Diese Überlappungen erlauben die forensische Verknüpfung von Angriffen.
- Angreifer benötigen Computer als Verteiler (distribution hubs) für ihre Malware, was zur Verwendung mehrerer Domainnamen führt. Jeder bekannte Domain-Name kann den Weg zurück zur IP-Adresse geben und gleichzeitig zum den Besitzer des Computers verweisen, wie unten gezeigt.

[3] vgl. Müller 2016, S.7

Es ist zu beachten, dass AS-Computer mit dem IANA-System nummeriert sind und jeder AS-Computer registriert ist. AS-Computer und die registrierten Personen/Organisationen können mit weiteren kostenlosen Tools wie *Ultratools* und vielen anderen Maschinen leicht abgefragt werden.
Für Domains und IP-Adressen existiert eine so genannte WHOIS-Registrierung, die oftmals mit kostenlosen Suchmaschinen verfügbar ist. Die Registrierungsangaben zeigen Firmennamen, Adressen, Telefonnummern und E-Mail-Adressen an. Dadurch wird der Schritt von der digitalen Welt zur physischen Welt gemacht, von Daten zu Personen und Organisationen. Damit kann der Forscher Einblick in das "digitale Ökosystem" von Servern, Adressen, Registrierungen, Domains etc. der Angreiferentität erhalten.

Auch gefälschte Registrierungsinformationen werden in Wirklichkeit oft wiederverwendet und ermöglichen es, Verbindungen zwischen bestimmten Angriffen herzuleiten. Überraschenderweise führt die Eingabe der Daten in Google oder jede andere Suchmaschine oft zu weiteren Erkenntnissen, die massiv die Chance erhöhen, Informationen zu finden, die sich auf eine Person mit einer realen Identität beziehen.

Reales Praxisbeispiel: 2013 hat die IT-Sicherheitsfirma *Mandiant* eine tiefgreifende Analyse chinesischer Cyberaktivitäten vorgelegt[4]. Später wurden 5 höhergestellte chinesische Militärs offiziell von den USA angeklagt, auch eine Person, die unter dem Decknamen **'***UglyGorilla***'** agierte. Diese Person hatte sowohl eine von APT1 genutzte IP-Adresse registriert wie auch ein im Netz zugängliches Personenprofil als Armeeangehöriger. China wies die Beschuldigungen zurück, aber US-Medien spekulierten, dass dieser Vorgang zu dem deutlichen Rückgang mutmaßlicher chinesischer Aktivitäten in den letzten beiden Jahren beigetragen hat[5].

Weiterhin reservieren größere Organisationen **IP-Blöcke**, z.B. Pakete mit aufeinander folgenden IP-Nummern[6]. Wenn eine vermutete IP-Adresse Teil eines solchen Blocks ist, kann dies helfen, auch alle anderen IP-Adressen in Domain-Suchmaschinen etc. zu überprüfen.

Reales Praxisbeispiel: Der Sicherheitsforscher *Krebs* wurde über eine IP-Adresse der *Carbanak*-Gruppe informiert, die 1 Milliarde US-Dollar durch Intrusion von Bankensystemen erbeutet hatte[7]. Seine Analyse der IP-Adress-Registrierung

[4] vgl. Mandiant 2013
[5] vgl. Mandiant 2013, Jones 2016, S.5, Nakashima 2016
[6] Es gibt noch weitere technische Optionen, wie z.B. die Vergabe virtueller **IP-Adressen** in Cloudbasierten Systemen und das Vortäuschen falscher IP-Adressen (**IP spoofing**), aber zumindest in den veröffentlichten Analysen von großen Cybercrime-Gruppen und Advanced Persistent Threats APT stellte dies kein Kernproblem dar.
[7] vgl. Kaspersky Lab 2015c

zeigte, dass der Firmenname auch für vergangene Cyber-Angriffe mit zwei anderen Arten von Malware verwendet wurde. Die E-Mail-Adresse führte ihn zu weiteren IP-Adressen der *Carbanak*-Gruppe. Die Telefonnummer erlaubte es *Krebs*, eine Person mit potenziellen Beziehungen zur *Carbanak*-Gruppe zu identifizieren; er war sogar in der Lage, diese Person zu kontaktieren[8].

Spezialisierte Angreifer haben schon darauf reagiert. Eine Strategie ist, IP-Adressen und Server schnell mit der sogenannten **Fast-Flux-Technologie** abzuwechseln. Auch das Herunterfahren bestimmter Server kann dann den Angreifer nicht stoppen. Eine Gegenstrategie ist jedoch die Verwendung von **Sinkhole-Servern**.
Wenn jemand eine Domain wie *www.example.com* in den Browser eingibt, muss der Computer die IP-Adresse des Ziels kennen. So genannte Domain Name Server (**DNS Server**) helfen dem Computer, die IP-Adresse zu finden.
Sinkhole-Server geben jetzt absichtlich falsche Hinweise (z. B. indem sie angeben, dass *www.example.com* die IP-Adresse 4.5.6.7 hat, während die wahre Adresse 1.2.3.4 ist) und damit den Datenverkehr von dem "echten" Computer wegleiten.
Der Sinkhole-Server kann die fehlgeleiteten Daten *erfassen und analysieren*. Da bei größeren Angriffen die Kommunikation für eine Weile im Gange ist, können sowohl Daten des Angreifers als auch die des Opfercomputers gesammelt werden, was hilft, die Probleme durch die sich ändernden IP-Adressen zu überwinden. Sinkholing wurde z.B. von der russischen Sicherheitsfirma *Kaspersky* gegen die vermutlich US-amerikanische *Equation Group* eingesetzt[9], die ihrerseits *Kaspersky* mit der anspruchsvollen Spionage-Malware *Duqu 2.0* infiziert hat[10].

Reales Praxisbeispiel: Das Ransomware-freisetzende Botnetz *Avalanche* nutzte die **Fast-Flux-Technologie**, um die Erkennung zu vermeiden. Schließlich erlaubte das Sinkholing, 130 Terabyte Daten abzufangen. Die Analyse dieser Daten erlaubte es den Strafverfolgungsbehörden, das Botnetz zu stoppen und die Mitglieder der *Avalanche*-Gruppe zu verhaften. Die Kooperation des *Bundesamtes für Sicherheit in der Informationstechnik BSI*, der Forschungseinheit *Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE*, der deutschen *Polizei*, *Europol*, *Eurojust*, des *FBI* und der Sicherheitsfirma *Symantec* machten dies trotz des Missbrauchs von 800.000 (!) Domains möglich[11].

Eine weitere Strategie ist die Verwendung von **Domains mit schwer nachverfolgbarer Registrierung**, die 2017 von der Sicherheitsfirma *Kaspersky* Labs für vermutete "Überlebende" der *Carbanak*-Gruppe gemeldet wurde. Einige

[8] vgl. KrebsonSecurity 2016
[9] vgl. Kaspersky Lab 2015a, S.34-35. Unerwarteterweise wiesen frühe Versionen der *Equation Group*-Malware hartcodierte (fest verankerte) IP-Addressen in ihren Programmen auf.
[10] vgl. Kaspersky Lab 2015b
[11] vgl. EUROPOL 2016

Länder erlauben den freien Verkauf von Domains mit ihrer Länderkennung wie Gabun (.ga) durch Anbieter wie *Freenom*. Jedoch hat jeder Provider das Risiko, von der nationalen oder ausländischen Polizei oder Nachrichtendiensten angegangen zu werden, um Zugang zu ihren Daten zu erhalten. Es gibt eine enorme weltweite Variabilität der Cybersicherheitsgesetze und Strafverfolgungsverfahren, und es gibt u.a. eine nie endende öffentliche Debatte und von Gerichtsverfahren in den USA, wer unter welchen Umständen befugt ist, Informationen über User von Privatunternehmen zu erfragen.

Der Dienst der Europäischen Kommission *European Commission Service* hat im Dezember 2016 einen Überblick über die aktuelle Rechtslage in den EU-Mitgliedstaaten veröffentlicht. Die Umfrage zeigte ein enormes Spektrum der Rechtsauffassungen, z.B. ob ein Anbieter mitwirken *kann* oder kooperieren *muss*, welches Ausmaß an Informationen angefordert wird, welche Arten von Strafverfolgungsmaßnamen verwendet werden (bis hin zum Fernzugriff auf Anbieter) und ob die Zusammenarbeit zwischen den Behörden praktiziert wird oder nicht[12].
Allerdings arbeitet die EU auf einen gemeinsamen Rechtsrahmen mit einem gemeinsamen Rechtsverfahren hin, der Europäischen Ermittlungsanordnung **European Investigation Order EIO** und die Europäische Union sieht Cybersicherheitsfragen als dringende politische Angelegenheit an.

Smart-Geräte haben eigene IP-Adressen. Die Analyse von Vorfällen mit intelligenten Geräten im Internet der Dinge (IoT) ermöglicht die Identifizierung des Herstellers und der beteiligten Produkte.

Reales Praxisbeispiel: Das Internet der Dinge (IoT) Botnetz *Mirai* nutzte Webcams, Babyphones und andere Geräte, um einen DDOS-Angriff auf den US-Internet-Infrastrukturanbieter *Dyn* mit Datenflussraten von mehr als 1 Terabit pro Sekunde im Oktober 2016 auszuführen. Die IP-Adressen führten zum Hersteller *Xiong Mai*.
Einige Tage zuvor hat ein Hacker mit dem Decknamen *Anna Sempai* 62 Passwörter für den Zugriff auf die Geräte freigegeben. Mittlerweile wurden von dem Sicherheitsforscher *Krebs* starke Anhaltspunkte gefunden, dass *Anna Sempai* an den *Mirai*-Vorläufern beteiligt war, insbesondere *QBot*, während für den Dyn-Angriff eine andere Gruppe *New World Hacker* die Verantwortung übernahm[13].
Später im Jahr 2016 wurde die deutsche Telekom massiv angegriffen. Hier wurde eine neue *Mirai*-Variante genutzt und die Analyse zeigte, dass wieder nur ausgewählte Geräte (sogenannte *Speedport*-Router) vom taiwanesischen Hersteller

[12] vgl. EU 2016
[13] vgl. KrebsonSecurity 2017, Radio Free Europe 2016

Arcadyan betroffen waren. Der Angriff schlug nur aufgrund eines Programmierproblems fehl[14].

2. Hacker

Die Cyberwelt kann in mehrere Akteurgruppen unterschieden werden:

- Der Staat mit Zivilbehörden, Militär- und Geheimdienste. Hacker können für diese Organisationen arbeiten, in einigen Staaten auch in staatlich verknüpften Hackergruppen.
- Cyber-Sicherheitsfirmen, die an der Erkennung, Zuweisung und Verteidigung beteiligt sind, aber auch beim Bau von Cyberwaffen und Spionagewerkzeugen. Hacker können auch als **Penetrationstester** fungieren, um Sicherheitsmaßnahmen einer bestimmten Einheit zu überprüfen.
- Im wissenschaftlichen und privatwirtschaftlichen Bereich können Hacker als **White Hat Hacker** arbeiten, um Sicherheitslücken zu finden und zu schließen, aber auch als **Black Hat Hacker** für kriminelle Zwecke oder zur Industriespionage der Industrie.
- **Hacktivisten** nutzen ihre Fähigkeiten für politische Aktivitäten.

Die oben genannten Sphären sind nicht vollständig getrennt. In Wirklichkeit kann ein begabter Hacker während eines Hacking-Contests prämiert werden, der dann vom Staat angestellt wird, um später irgendwann in den privaten Sicherheitsbereich zu wechseln[15].

Während das ursprüngliche Image der Hacker mehr anarchisch war, sind mittlerweile Staaten intensiv und routinemäßig auf der Suche nach erfahrenen Hackern, um sie zu anzuwerben. **IT-Summer Camps, Hackerwettbewerbe, Hackathons** (Hacker-Marathons, wo ein bestimmtes Problem gelöst werden muss) sind typische Aktivitäten. Die Suche nach Hackern ist aber nur ein kleiner Teil der Suche nach qualifizierten IT-Mitarbeitern im Allgemeinen: Qualifizierte IT-Studierende können auch direkt von Staaten und Sicherheitsfirmen kontaktiert werden.

Auch die Rekrutierungsmethoden seitens der Nachrichtendienste und des Militärs haben sich deutlich weiterentwickelt. Studien zeigen, dass Hacker trotz der ursprünglichen Distanz unter Umständen für den Staat zu arbeiten bereit sein

[14] vgl. Alvarez/Jansen 2016. (Nachtrag: Am 22.02.2017 wurde am Londoner Flughafen ein 29-jähriger Brite verhaftet, der verdächtigt wird, den Hack begangen zu haben. An der Aktion waren deutsche, britische und zypriotische Behörden beteiligt).
[15] vgl. Rosenbach 2016, Kramer 2016

können[16]. Im Ergebnis konnten die Rekrutierungsmethoden in der Cybersicherheit inzwischen einfacher gestaltet werden[17].

Der typische Hacker ist ein jüngerer Mann, der - wenn er in größere Cyber-Attacken involviert ist - dies als regelmäßigen Job macht. Die Dominanz der jüngeren Männer im Hacking spiegelt die Dominanz der jüngeren Männer im IT-Bereich im Allgemeinen wider. Dies wird mittlerweile als ein Problem gesehen, da dies die unzureichende Resourcennutzung von Frauen im IT-Bereich anzeigt. Der britische Cyber-Nachrichtendienst *Government Communication Headquarter GCHQ* ist nun systematisch auf der Suche nach qualifizierten Frauen durch die Initiierung der *CyberFirst Girls Competition* für 13 bis 15 Jahre alte Mädchen mit Tests in Kryptologie, Logik und Codierung. Ende Februar 2017 starten 600 Teams den Wettbewerb. Derzeit sind nur 37% der 12.000 Mitarbeiter im britischen Geheimdienstsektor Frauen.[18]

Der typische Hacker ist kein Einzelkämpfer, sondern interagiert mit Freunden und anderen Hackern, um Werkzeuge und Erfahrungen auszutauschen, Einblicke und Neuigkeiten aus der Szene zu bekommen usw. Dies geschieht mit Decknamen in **Hackerforen**, auf dem **Schwarzmarkt** und im **Darknet**[19]. Diese drei Bereiche überlappen sich gegenseitig. Manchmal gibt es auch **defacement websites**, wo Hacker Screenshots der gehackten und beschädigten (verunstalteten) Webseiten als eine Art Trophäe posten.

Dies öffnet den Weg zur Attribution: Decknamen können in mehreren Angriffen erscheinen, auch die verwendeten E-Mail-Adressen. Wenn ein einzelner Hacker einen Angriff öffentlich für sich beansprucht, steigt das Risiko, gefasst zu werden, wie z.B. der Hacker mit dem Decknamen *Anna Sempai*, der an den *Mirai*-Botnet-Attacken beteiligt war und der wahrscheinlich schon identifiziert wurde[20].
Wieder kann es hilfreich sein, den Decknamen eines Hackers in eine Suchmaschine einzugeben, um weitere Hinweise zu erhalten. Die Praxis zeigt, dass Hacker manchmal mehrere Decknamen verwenden, *aber nicht zu viele*, denn sonst verlieren sie ihr "Profil" in der Insider-Szene.

---

[16] vgl. Zepelin 2012, S.27. Krasznay 2010 zitiert bei Chiesa 2012, Folie 69.
[17] vgl. Zepelin 2012, S.27. Der offene Ansatz kann wie folgt illustriert werden: Wenn man seit 2012 in den USA Suchbegriffe zum Thema cyberwar auf der Seite startpage.com eingab (ein Service, der anonyme Suche bei Google erlaubt), konnte es passieren, dass auch eine gesponserte Anzeige der National Security Agency NSA erschien (ebenso bei *ixquick* und *metacrawler*). Diese bot Cyberkarrieren unter dem Link www.nsa.gov/careers an mit der Zeile "*National Security Agency has cyber jobs you won't find anywhere else!*". Im Jahr 2016 ist die Anzeige verfügbar unter intelligencecareers.gov/nsa. Die CIA hat ebenfalls eine eigene Suchmaschinenanzeige kreiert "*CIA Cyber careers – The work of a Nation – cia.gov The Center of Intelligence –Apply today*" und hat seit Juni 2014 einen eigenen offiziellen Twitter-Account.
[18] vgl. Wittmann 2017
[19] Eine Übersicht findet sich bei Chiesa 2015
[20] vgl. KrebsonSecurity 2017

Reales Praxisbeispiel[21]**:** In der *Winnti 2.0*-Attacke trug eine Bot-Kommunikation via *Twitter* als Header den Decknamen eines der Hacker, der sich dann auch in Hacker-Foren finden ließ. Dort hatte er E-Mail-Kommunikation mit einem Freund, der eine reguläre Social-Media-Website mit allen Kontaktdaten hatte. Auch eine Abkürzung im Malware-Programm führte zu weiteren Treffern in Suchmaschinen und führte zu einem Hacker-Team, von dort wiederum zu einer Mail-Adresse, die dann wieder zu einer jungen männlichen Person führte.

Das Darknet wurde in den Medien 2016 und 2017 als großes Problem thematisiert. Das TOR-System (abgeleitet von *The Onion Router*) gilt in den Medien als Rückgrat des Darknet, weil es die Aufteilung von Datenpaketen über mehrere Strecken und damit einen hohen Grad an Anonymität im Netz ermöglicht.

Allerdings gerät TOR zunehmend unter Druck. Eine neuere Arbeit des *Naval Research Laboratory*, das das TOR-System ursprünglich erfunden hat, zeigt, dass die Übernahme eines autonomen Systems oder eines IXP-Knotencomputers (siehe oben in Abschnitt 1) durch einen Gegner genügend Informationen zur Erfassung eines Nutzers innerhalb von Wochen oder manchmal sogar innerhalb von Tagen bereitstellen würde[22]. Während dieses Erkennungsverfahren nur als statistische Modellierung präsentiert wurde, zeigt die Arbeit, dass das TOR-System wohl nicht auf Dauer eine Barriere gegen Erkennung und Attribution bleiben wird.

In Bezug auf das Darknet sollte man bedenken, dass die Akteure auch Undercover-Ermittler sein können[23].

[21] vgl. Kaspersky 2013, S.53ff.
[22] vgl. Johnson et al. 2013
[23] vgl. Tellenbach 2017, S.31

3. Schadsoftware (Malware) und Advanced Persistent Threats (APTs)

3.1 Hochentwickelte Hackereinheiten und Malware-Programme

Mittlerweile wurden mehrere hochentwickelte Hackergruppen und Malwarefamilien entdeckt und berichtet, die in den folgenden Abschnitten dargestellt werden. Typischerweise geht man davon aus, dass diese Gruppen zu Staaten (Regierungen/Nachrichtendienste/Militär) gehören bzw. von diesen unterhalten werden. Gründe für diese Annahme sind der betriebene Aufwand und die Komplexität der verwendeten Instrumente, der Bedarf an Spezialisten, die diese Operationen über Jahre durchführen und zugleich verbergen müssen, die Auswahl von politisch und strategisch besonders wichtigen Zielen, der Bedarf an systematischer Sammlung von Informationen usw. Außerdem sind diese Attacken typischerweise nicht sofort profitabel, im Unterschied zu Cyberkriminellen, die Geld mit Bankingtrojanern, Ransomware und ähnlichem verdienen können.
Zudem hat jede dieser Gruppen ein charakteristisches Muster von Zugangswegen, ausgenutzten Schwachstellen und Werkzeugen, was diese Gruppen unterscheidbar macht.24. Ein weithin genutzter Begriff für diese Muster ist **Tactics, Techniques, and Procedures (TTPs)**. Da jede Gruppe auch zu bestimmten Zielen tendiert, spricht man auch von einer Opferlogik, engl. **victimology**.

Die Angriffstaktik variiert: Führende Techniken sind **Phishing-E-Mails** mit infizierten Anhängen oder Links zu infizierten Websites. Wie in der *APT28/Fancy Bear*-Analyse der Sicherheitsfirma *FireEye* skizziert, können solche E-Mails auch zur Spurensuche verwendet werden, wie z.B. "spezifische E-Mail-Adressen, bestimmte Muster, spezifische Namensdateien, MD5-Hashes, Zeitstempel, benutzerdefinierte Funktionen und Verschlüsselungsalgorithmen"[25].

Die Verwendung **gestohlener Sicherheitszertifikate** und die Verwendung von **Zero-Day-Exploits** sind typische Indikatoren für eine anspruchsvolle Angreifergruppe.

Jedoch müssen Zuordnungen zu Staaten mit großer Vorsicht gehandhabt werden. Manchmal werden falsche Fährten (**false flags**) gesetzt, oder es wird Malware verwendet, die bereits auf dem Schwarzmarkt erhältlich ist. Manchmal sind Cyberwaffen wenn auch unter Auflagen sogar kommerziell erhältlich.
Zudem hat noch keine Regierung oder Behörde eine Verbindung zu einer Hackereinheit offiziell bestätigt. Eine ‘Verbindung’ zu einem Staat ist zudem ein

[24] Siehe auch Jennifer 2014
[25] vgl. FireEye 2014, S.29

unscharfer Begriff, man kann daraus nicht erkennen, ob eine Einheit Teil einer staatlichen Organisation ist oder lediglich mit diesem auf Vertragsbasis arbeitet oder anderweitig kooperiert. Die nun vorgestellten Gruppen sind die meistberichteten in den Medien, jedoch wird die Nummer größerer aktiver Hackereinheiten auf rund hundert Gruppen geschätzt.

Aus amerikanischer Sicherheitsperspektive hat Russland innerhalb der letzten zehn Jahre erhebliche Fortschritte mit der Errichtung hochspezialisierter Einheiten gemacht. Während die Gruppen *APT28, APT29* und *The Waterbug Group* inzwischen von vielen Analysten Russland zugeschrieben werden, ist die Debatte über mögliche Verbindungen zu Russland offen für Gruppen mit dem Fokus auf Industrie und ICS-Systeme wie *Energetic Bear/Dragonfly* und *Sandworm/Quedagh*[26].
Die *Comment Crew/APT1* und die *Axiom/DeepPanda Group* werden im Zusammenhang mit China diskutiert, während für die *Lazarus Group* ein Zusammenhang mit Nordkorea vermutet wird. Die *Equation Group* wird typischerweise mit den USA in Verbindung gebracht, wobei Bezug zu den sogenannten *Snowden leaks* genommen wird. Aber es gilt unbedingt zu beachten, dass alle angesprochenen Regierungen solche Verbindungen verneint bzw. nicht kommentiert haben.

Alle führenden Gruppen haben mehrere Namen, denn Analysten weisen einer Gruppe typischerweise einen Arbeitsnamen zu und es erweist sich erst später, dass dieselbe Gruppe von verschiedenen Analysten adressiert wurde. Auch Cyber-Sicherheitsfirmen haben interne Namenskonventionen, wie z.B. *Bear* = vermutlich Russisch, *Panda* = vermutlich Chinesisch und so weiter. Manchmal lösen Codes oder Begriffe in der Malware die Benennung aus, z.B. der Name *Sauron* in der kürzlich entdeckten APT *Project Sauron* (das all-sehende böse Auge aus *Herr der Ringe*). Es ist wichtig für die Attributionsforschung, diese Aliasnamen zu kennen, um Wissen aus verschiedenen Quellen richtig zu kombinieren.

Reale Praxisbeispiele: *APT 28* ist auch bekannt als *Sofacy, Pawn Strom, Csar Team, Sednit, Fancy Bears* oder *Strontium, APT 29* als *Cozy Bears* oder *The Dukes*, die *Axiom Group* ist auch bekannt als *DeepPanda, Shell_Crew, Group 72, Black Vine, HiddenLynx, KungFu Kittens etc.*

Im Augenblick sind die meist diskutierten Cybercrime-Gruppen die *Carbanak Gruppe* und das *Avalanche* Botnetz.

[26] Siehe z.B. Jennifer 2014

3.2 Analyse der Malware

Hochentwickelte Schadprogramme (**Malware**) sind Softwareprogramme, mit deren Hilfe man andere Computer angreifen, infiltrieren, ausspionieren und manipulieren kann und die ihre Ausbreitung selbsttätig steuern können. Derartige Programme nehmen an Häufigkeit zu, so dass die bisherige Einteilung in Viren, Würmer und Trojanern langsam an Bedeutung verliert. Die höchstentwickelten Programme weisen technische Gemeinsamkeiten auf:
Anfangs wird nur ein kleines Programm geladen, um das Eindringen zu erleichtern. Um einer Entdeckung vorzubeugen, führt das Schadprogramm Schritte zur **Selbstverschlüsselung** durch und bereitet eine Option zur **Selbstlöschung** vor, die nach Abschluss der Cyberspionage-Operation genutzt werden kann. Zum letzteren gehört ggf. auch die Fähigkeit, **sich selbst abschalten** (stilllegen) zu können. Danach wird weitere Malware geladen in Abhängigkeit von der vorgefundenen Information. Anstatt große Schadprogramme zu kreieren, werden mittlerweile variable Module nachgeladen, die passgenau an die Zielperson und die Computerumgebung angepasst sind. Die fortgeschrittensten Programme erlauben eine mehr oder minder totale Kontrolle des Computers und einen Zugriff auf alle Daten. Die Speicherung der Malware und ggf. der Information findet an ungewöhnlichen Orten wie der Registry oder sogar der in der Hardware befindlichen Firmware statt, um so eine Entdeckung, aber auch eine Entfernung vom Computer zu blockieren. Ein typischer Schritt besteht darin, sich über User ohne besondere Rechte zu Administratorenrechten hochzuarbeiten (**lateral movement**).

Dies resultiert in einem **Advanced Persistent Threat (APT)**, d.h. dem dauerhaften Zugang nicht-autorisierter Personen zu einem Netzwerk. Die Analyse der Malware wird durch falsche Spuren (**false flags**) erschwert, bei denen irreführende Zeitstempel und Spracheinstellungen in dem zur Programmierung genutzten Computer verwendet werden, zudem werden Code-Bruchstücke, die auf andere Hackergruppen hinweisen, eingebaut. Derartige Fälschungen bergen ein hohes Fehlerrisiko, in größeren Malwareprogrammen kann es passieren, dass einzelne Zeitstempel oder Spracheinstellungen nicht durchgehend geändert wurden.
Zudem hinterlassen Hacker auch **digitale Fingerabdrücke**, womit man charakteristische Zugriffsmuster oder Programmcodes bezeichnet. Diese erlauben eine Differenzierung zwischen Angreifergruppen[27].
Diese Zugriffsmuster können sich ggf. auf **malware families** (verwandte Arten von Schadsoftware), die Nutzung von bestimmten Werkzeugen oder Werkzeugkombinationen, Zielrichtung des Datendiebstahls, Nutzung bestimmter

[27] vgl. Mayer-Kuckuck/Koenen/Metzger 2012, S.20-21

Verschlüsslungen, Nutzung verdeckter Kommunikation zu Kontrollrechnern des Angreifers (z.B. durch Vortäuschung legitimen Datenaustauschs) und der benutzten Sprache (inkl. Schreibfehlern, -stil, bevorzugten Begriffen etc.) beziehen [28]. Informationen können auch in kleinen Bildern verborgen werden, einer als **Steganographie** bekannten Methode. benutzte Manchmal benutzen Angriffsserver *Twitter* oder e-mail zur Kommunikation mit dem Zielcomputer.

Reales Praxisbeispiel: Anfang 2015 berichtete die Sicherheitsfirma *Kaspersky Labs* über eine neue Malware-Familie, die sich *Equation group* nennt. Die Malware kann bis 2001 zurückverfolgt werden, eventuell sogar bis 1996. Aufgrund technischer Überlappungen könnte es sein, dass *Stuxnet*, das gegen Uranzentrifugen im Iran eingesetzt wurde, Teil einer größeren Malware-Familie ist.[29]. Die *EquationGroup* Malware-Familie umfaßt die Programme *EquationLaser*, *EquationDrug*, *Grayfish*, *Fanny*, *Double Fantasy* and *TripleFantasy***,** während die zu *Stuxnet* gehörende Familie *Stuxnet*, *Flame*, *Duqu* und *Gauss* (mit den Abkömmlingen *MiniFlame* und *Duqu 2.0*[30]) umfaßt. Wichtige Verbindungen zwischen der *EquationGroup* Malware-Familie und der *Stuxnet*-Familie sind die folgenden[31]: *Grayfish* nutzt in einem Infektionsschritt eine Hash-Code Verschlüsselung, die Ähnlichkeiten zum *Gauss*-Programm aufweist. *Fanny*, *Stuxnet*, *Flame* und *Gauss* nutzen einen gemeinsamen LNK-exploit, während *Fanny*, *Stuxnet*, *DoubleFantasy* und *Flame* eine bestimmte Methode zur Eskalation von Nutzerprivilegien verwenden. Zudem nutzen *DoubleFantasy*, *Gauss* und *Flame* noch eine spezifische Methode der USB-Infektion.

Inzwischen werden die **Programmierstile** von Programmieren gesammelt und ausgewertet, so dass neue Softwareprogramme mit älteren abgeglichen werden können (‘**Stilometrie**’). Die NSA untersucht z.B. die Art und Weise, wie Klammern gesetzt, Variablennamen benutzt und Leerstellen gesetzt werden und die Struktur des Programmiertexts. Programmtexte werden z.B. während Hackercamps gesammelt oder auch Arbeiten von Informatikstudenten. Jedoch nimmt die Nutzung von Verschleierungssoftware (**obfuscation software**) zur Ersetzung von Namen und Veränderung von Klammern zu[32]. Wichtig ist jedoch, dass selbst eine erfolgreiche Abgrenzung einer bestimmten Gruppe von Angreifern noch keine Auskunft darüber gibt, ob diese im Dienste eines Staates stehen.

Reales Praxisbeispiel: In 2016 unternahmen IT-Sicherheitsfirmen mit Firmen wie *Symantec, Kaspersky, Alien Vault* etc. unter Führung von *Novetta* die *Operation*

[28] vgl. Mandiant 2013
29 vgl. Kaspersky Lab 2015a, S.3
[30] vgl. Kaspersky Lab 2015b, S.3
[31] vgl. Kaspersky Lab 2015a S.5
[32] vgl. Welchering 2016, S.T4

Blockbuster, um Fälle von Cyberspionage und Wiper-Attacken in Korea und den USA zu analysieren wie auch den sog. *Sony Pictures Entertainment (SPE)*-Hack von 2014. Die gemeinsame Analyse ergab starke Hinweise, dass zumindest zwei der drei großen Wiperattacken und der *Sony/SPE-Hack* von derselben Gruppe, die nun *Lazarus-Gruppe* genannt wird, durchgeführt wurden.
Novetta identifizierte 45 Malwarefamilien mit vielen Beispielen von **wiederwendetem Code** und **überlappender Programmierung**. Das schloss auch recht spezielle Anwendungen wie ähnliche **Suicide Scripts** ein, mit denen man Malwareprogramme nach erfolgreicher Ausführung wieder entfernen kann und ein typisches **space-dot-encoding**, bei dem Begriffe, die von Sicherheitssoftware erkannt werden können, durch unnötige Leerstellen und Symbole gespreizt werden. Die Programme enthielten auch besondere Rechtschreibfehler wie 'Mozillar' statt ‚Mozilla' in mehreren Malwarefamilien und außerdem wurde für verschiedene Malware-Dropper **dasselbe Passwort wiederverwendet**.

Allerdings war der SPE-Hack eine der umstrittensten Debatten in der Cyber-Attributions-Geschichte, die sich aus unerwarteten Fakten wie die anfängliche Geldforderung, Datenverteilung von Computern außerhalb Nordkoreas usw. ergab.[33][34]. Auch die Mischung aus Cyberspionage und verdächtigen cyberkriminellen Aktivitäten wie der Angriff auf das Interbanken-System SWIFT war irritierend[35].
Allerdings könnten die meisten Widersprüche gelöst werden, wenn die folgenden Annahmen richtig sind:
1. Der SPE-Hack war zunächst ein Fall von Cyber-Kriminalität, der zu einem späteren Zeitpunkt zur politischen Materie eskalierte. Dies würde dem Kommunikations- und Angriffsmuster entsprechen.
2. Die *Lazarus*-Gruppe hat einen Kern von staatlich gebundenen Hackern, die Hacker in Südostasien koordinieren. Dies würde seltsame Befunde wie die langen Arbeitszeiten, die Angriffsorte, aber auch die Frage der begrenzten Netzwerkkapazitäten usw. erklären.

Der SWIFT-Interbanking-Angriff ist von besonderer Bedeutung, denn inzwischen hat sich gezeigt, dass sowohl die *Lazarus*-Gruppe als auch zu *Carbanak*-gehörende Hacker **unabhängig voneinander das gleiche Ziel** angegriffen haben. Der Wiper-Code, der von der *Lazarus*-Gruppe benutzt wurde, um die Bankhacks zu verschleiern, war identisch zu dem, der im SPE-Angriff verwendet wurde[36], während die mutmaßlichen *Carbanak*-Hacker letztere eine neue Malware namens *Odinaff* benutzten[37].

[33] vgl. Fuest 2014b, S.31
[34] vgl. The Security Ledger online 2014, S.1
[35] vgl. Brächer 2016, S. 26-27
[36] vgl. Storm 2016
[37] vgl. Symantec 2016c

Viele Menschen betrachten Intrusion als statisches Ereignis: Sobald die Malware installiert ist, kann sich der Angreifer zurücklehnen und der Datenfluss läuft von allein.
In Wirklichkeit ist ein Cyberangriff ein **dynamischer Prozess**. Der Angreifer kann versuchen, die Zugangs- und Kontrollrechte zu erweitern oder durch eine **lateral movement**, d.h. zu anderen Computern der eingedrungenen Organisation zu gelangen. Es müssen Updates erstellt und maßgeschneiderte Module hochgeladen werden. Anleitungen müssen an den Zielcomputer gesendet werden.
Eindringlinge müssen darauf achten, dass sie nicht entdeckt werden, z.B. durch Veröffentlichung eines von ihnen verwendeten Exploits. Die extrahierten Daten müssen sorgfältig analysiert werden, um weitere Bedürfnisse zu identifizieren oder zu realisieren, wenn ein weiterer Angriff eine Verschwendung von Zeit und Ressourcen ist.
Deshalb ist es schwierig, den Angriff einer APT zu imitieren, auch wenn die Malware der jeweiligen Hackergruppe auf dem Schwarzmarkt verfügbar ist. Der Angreifer muss sich bewusst sein, dass die Cyber-Security-Unternehmen ihr Wissen nicht zur Gänze veröffentlichen, dass die Nachrichtendienste des Mitgliedsstaates auch mehr über die Nutzung wissen und natürlich die ursprüngliche Hackergruppe ihre Malware besser als jeder andere kennt und daher nicht nur am besten weiß, *was* benutzt wird, sondern auch *wie* und *wann*.

Reales Praxisbeispiel: Es gab Überlappungen zwischen den Attacken von A*PT28/Fancy Bears* auf den *französischen TV-Sender TV5Monde*, den *Bundestag* and die *US Democratic National Convention DNC*.
Der Angriff auf den Bundestag wies Ähnlichkeiten zum Angriff auf den französischen TV-Sender TV5Monde auf[38]. Einer der für die Attacke auf den Bundestag genutzten Server war identisch zu denen der DNC-Attacke von 2016 und ebenso ein gefälschtes Sicherheitszertifikat[39].
Allerdings könnte eine Angreifergruppe natürlich Malware verwenden, die auf dem Schwarzmarkt verfügbar ist, aber selbst dann kann die Gruppe **typische Charakteristika** und Programme im Einsatz zeigen.

Reales Praxisbeispiel: Die *Axiom-Gruppe* führt hochentwickelte Phishingattacken durch Aufsatteln auf laufende reale Konversationen (**piggybacking**) durch, um das Opfer zum Anklicken von infizierten Links zu motivieren[40]. Die Malware *Zox* und *Hikit* wurden nur bei Axiom beobachtet,

38 vgl. FAZ online 2015, siehe auch Wehner 2015, S.1
39 vgl. Baumgärtner/Neef/Stark 2016, S.90-91
40 vgl. Alperovitch 2014

während andere verwendete Malwareprogramme auch von anderen Organisationen genutzt werden[41].

Spezialisierte Hacker-Einheiten (z.B. die *Equation Group* and *Waterbug Group*) können Computer **auf bereits vorhandene Infektionen** mit ihrer Malware **überprüfen** und wenn sie Infektionen von Computern erkennen, die bisher weder angegriffen noch infiziert wurden, werden sie benachrichtigt. Die Hacker-Einheiten könnten sogar in der Lage sein, den Angriff unter falscher Flagge direkt zu untersuchen und dann hat der imitierende Angreifer sowohl in der digitalen als auch in der physischen Welt massive Probleme.

Reales Praxisbeispiel: Die Multifunktionsmalware namens **Uroburos/Turla/Snake/Carbon**, die als rootkit arbeitet, ist in der Lage, innerhalb eines Intranets ein eigenes Peer-to-Peer Netzwerk aufzubauen und weist viele technische Überlappungen zu **agent.btz/Trojan Minit**[42] auf, die ein Eindringen in Pentagon-Computer über USB-Sticks ermöglichte. In diesem Netzwerk sucht *Uroburos* dann einen Computer, der doch mit dem Internet verbunden ist, um dann den Datenaustausch zu beginnen. *Uroburos* wird nicht aktiv, wenn der Computer bereits mit der Malware *agent.btz* befallen ist, was auf einen gemeinsamen Ursprung hindeutet[43].

Zusätzlich zu den obigen Analysen ist die **Chronologie** der Malware-Entwicklung wichtig, um zu erkennen, welche Malware aus Vorläufern abgeleitet werden und damit mit denselben Angreifern zusammenhängen könnte. Für alle anspruchsvollen Malware-Gruppen existiert eine solche Chronologie. Es ist erwähnenswert, dass z.B. die Stuxnet-Malware nicht nur eine lange Versionsgeschichte hatte, sondern dabei auch massive Veränderungen ihrer Struktur und Ziele (ursprünglich Klappenschluß, später Urangaszentrifugen) erfuhr. [44]

Reales Praxisbeispiel: Die neue APT *Project Sauron* (auch bekannt als *Strider*) wurde im Jahr 2016 entdeckt, aber die Malware-Eigenschaften zeigen an, dass die Programmierer von anderen anspruchsvollen Malwareprogrammen gelernt haben, insbesondere von *Duqu, Flame* (Verwendung der Programmiersprache *Lua*), *Equation* und *Regin*, aber schon zu einer Zeit, wo diese Malware-Typen noch

[41] vgl. Novetta 2015, S.20. Jedoch wies *Novetta* in der Analyse der *Winnti-Gruppe* im Rahmen der Operation SMN darauf hin, dass *Hikit* nun genutzt wurde, um *Winnti*-Attacken zu unterstützen. Ob dies nun bedeutet, dass die *Hikit*-Malware nicht mehr exklusiv ist oder *Winnti* (deren Fokus von der Spieleindustrie zu anderen Branchen gewechselt hat wie *ThyssenKrupp*) nun mit *Axiom* verbunden ist, ist nicht klar.
[42] vgl. Symantec 2016a, S.10-11
[43] vgl. Fuest 2014a, S.1-3
[44] vgl. McDonald et al. 2013, S.1-2

nicht entdeckt waren, was auf eine Beziehung zwischen den APTs hindeuten kann[45].

Im Bereich der Cyerkriminalität endet ein Cyber-Angriff nicht mit der Computer-Kommunikation, sondern das Geld, das durch die Angriffe gewonnen wird, muss übertragen und versteckt werden. Diese **Geldwäsche** wird in der Regel mit mehreren Transfers zwischen Bankkonten durchgeführt, um den Ursprung des Geldes zu verschleiern. Die **Verwendung von digitalen Bitcoins** löst das Problem nicht wirklich, denn am Ende müssen die Bitcoins dann doch wieder in echtes Geld umgetauscht werden. Die Übertragung von großen Geldsummen und schnelle Konto-Bewegungen sind Warnsignale.
Menschen, die ihr Bankkonto für Geldtransfers nutzen, sind die sogenannten **money mules**, d.h. neben den Hackern sind weitere Personen Teil der Cyberkriminalität. Experten identifizierten die Geldwäsche bei Cyber-Verbrechen als eine wichtige Schwachstelle der Angreifer[46].

3.3 Erkennung und Vorbeugung von Angriffen

Mittlerweile kann die Angriffserkennung auch eine Echtzeit-Attribution sein.

Threat Intelligence Repositories vergleichen eingehende Informationen mit bekannten IP-Adressen, Domainnamen, Webseiten und auch mit Listen bekannter bösartiger Attachments[47]. Dies ermöglicht eine sofortige Erkennung und manchmal sogar die Zuordnung eines eingehenden Angriffs. Neu entdeckte Malware kann mit so genannten **Indicators of Compromise IOC** integriert werden, d.h. Zahlenfolgen, die die Erkennung der Infektion in einem bestimmten Computer ermöglichen.

Zusätzlich zu den üblichen Empfehlungen zur Cyberabwehr wie der Nutzung starker (schwer zu erratender) Passwörter, aktualisierten Systemen, vorsichtigem Verhalten im Internet, Vermeidung verdächtiger e-mails und Anhänge usw. wird die automatisierte Erkennung von Angriffen immer mehr verstärkt.

Die US-Regierung baut im Moment hochentwickelte Sensorsysteme aus[48]: Das **Continuous Diagnostics and Mitigation (CDM)**-Programm kann abnormes Verhalten in Echtzeit erkennen und entsprechende Übersichtsberichte an Administratoren erstellen.

---

[45] vgl. Kaspersky 2016, S.21, Symantec 2016b
[46] vgl. Baches 2016, S.15
[47] vgl. Alperovitch 2014. Die IT-Sicherheitsfirma *CrowdStrike* nutzt den auf Windows und Mac-Servern, Desktops und Laptops eingesetzten Kernelsensor *Falcon host* zum Erkennen von Angriffen und dem Abgleich mit einer Datenbank (threat intelligence repository) für die Attribution.
[48] vgl. Gerstein 2015, S.4-5

Einstein 3A arbeitet mit Sensoren an Webzugangspunkten, um Bedrohungen aus dem zu schützenden System herauszuhalten, während das CDM Bedrohungen identifizieren soll, wenn sie schon im System sind.

US-Forscher haben Mustererkennungsalgorithmen zur Cyberabwehr entwickelt, die im Falle eines erkannten Angriffes die Löschung von Datenpaketen des Angreifers erlauben. Zur Vermeidung von Eskalationen ist jedoch keine automatisierte Vergeltung vorgesehen. China erforscht Simulationen von Cyberattacken[49].

Zu diesem Zweck hat die Deutsche Telekom 200 **Honeypot** ('Honigtopf')-Computer in ihrem Netz installiert, die durchschnittliche Mobiltelefone und Computer simulieren. Diese Computer erfassen jede Aktivität des Angreifers[50], das Analysesystem wird auch als Sandkasten (**sandbox**) bezeichnet. Da fortschrittliche Malware in virtuellen Maschinen (Testumgebungen) inaktiv bleibt, versuchen fortschrittliche sandboxes echten Computern so gut wie möglich zu ähneln. Jedoch ist Malware ggf. durch das sogenannte **code morphing** geschützt, das ist eine Verschleierungsmethode, um Software gegen Nachbau durch reverse engineering, Analysen, Modifikationen und Codeknacken (cracking) zu schützen.

Einen bedeutenden Fortschritt stellt die Bildung von **Cyber-Allianzen** dar, z.B. die *Cyber Threat Alliance* der Sicherheitsfirmen *Fortinet, Intel Security, Palo Alto Networks* und *Symantec* zur Bekämpfung von Ransomware. Eine wachsende Zahl privater Sicherheitsfirmen sammelt Daten und führt Langzeitanalysen zur Identifikation von Angreifern durch. In schwierigen Fällen tendieren die Firmen auch zur Kooperation und zur Kombination ihrer Analysen, z.B. in den großangelegten cyberforensischen Operationen *SMN* und *Blockbuster*, Einzelheiten folgen weiter unten.
Da die ausgefeiltesten Attacken typischerweise von Gruppen ausgeführt werden, die über mehrere Jahre operieren und nicht etwa als isolierte 'Hit and run'-Angriffe, werden die Anstrengungen zur Attribution immer effektiver. Auch große Privatunternehmen koordinieren ihre Cyberverteidigung, wie z.B. in der *Deutschen Cyber Sicherheitsorganisation DCSO* mit *VW, BASF, Allianz und Bayer*.

3.4 Human Intelligence (HumInt)

Die Identifikation der Angreifer ist mit rein digitalen Methoden manchmal unmöglich. Die Anwendung von Spionagemethoden der Human Intelligence kann dazu beitragen, den *missing link* zu finden.

[49] vgl. Welchering 2014, S.T4
[50] vgl. Dohmen 2015, S.75

Die folgenden Methoden sind in der Praxis der Attribution die wichtigsten:

- Cyber-Intelligence
- Intelligence Cooperation zum Informationsaustausch
- Konventionelle Anwendung von Intelligence.

3.4.1 Cyber-Intelligence

Ganz generell läßt sich sagen, dass viele Firmen einschließlich von IT-Sicherheitsanbietern Informationen über Sicherheitslücken an die Geheimdienste weitergeben, bevor diese veröffentlicht bzw. geschlossen werden, um so die Geheimdienstarbeit zu unterstützen[51]. Nutzer von Geräten, Software und IT-Sicherheitsanwendungen müssen also davon ausgehen, dass der Geheimdienst des jeweiligen Herstellungslandes *eventuell* einen Zugang hat und nutzt, dass dies über Geheimdienstkooperationen *eventuell* auch indirekt für die Dienste anderer Staaten gilt und ein zero day-exploit eventuell keineswegs 'zero' ist. Zusammen mit der Überwachung des Informationsflusses[52] und dem oben beschriebenen Zugang zu Verschlüsselungssystemen, kann auch die Cybersicherheit *zwischen* Computern ein Problem sein. Mittlerweile hat die US-Regierung die Nutzung von Exploits offiziell bestätigt, wobei die Entscheidung hierzu nach einer sorgfältigen Risiko-Nutzen-Abwägung erfolgt, d.h. wer könnte noch davon wissen, wie groß ist das Risiko der Entdeckung, welchen Schaden könnten die eigenen User und Firmen nehmen[53].

Die Vorbereitung des Schlachtfeldes (*Preparing the battlefield*) gilt als wesentlich für erfolgreiche Strategien, in der Praxis werden vorsorglich Sender (**beacons**) oder Implantate in ausländischen Computernetzwerken platziert, das ist Computercode, mit dessen Hilfe die Arbeitsweise des Netzwerks untersucht werden kann[54].

Ein weiteres Problem ist der **Zugriff vor der Verschlüsselung**, da manche Provider verschlüsselte Nutzerdaten für die interne Verarbeitung entschlüsseln und anschließend wieder verschlüsseln. Durch den Zugriff auf solche Zentralrechner können Angreifer die Verschlüsselung also umgehen.

---

[51] vgl. FAZ 2013, S.1

[52] Dies schließt die konventionelle Überwachung papierbasierter und analoger Kommunikation wie auch das Abhören von Daten aus Glasfaserkabeln mit ein, vgl. Gutscher 2013, S.7, Welchering 2013, S.6. In Überstimmung mit den jeweils gültigen nationalen Gesetzen, wie z.B. dem 1994 **Communications Assistance for Law Enforcement Act (CALEA)** und dem **Foreign Intelligence Surveillance Act (FISA)** in den USA, geben Provider ggf. Zugang zu Daten oder Systemen.

[53] Daniel zitiert von Abendzeitung 2014

[54] vgl. Sanger 2015, S.5

Reales Praxisbeispiel: Aus diesem Grunde waren schon 2010 mehrere Staaten an den Blackberry-Provider *Research in Motion (RIM)* herangetreten, Server in ihren Ländern zu installieren[55]. Doch inzwischen werden viele Anbieter auf der ganzen Welt mit Anfragen von vielen Ländern konfrontiert, einen Server in einem bestimmten Land aufzustellen; das ist mittlerweile Normalität, die die Kontrolle über den Datenfluss und die Attribution viel einfacher macht. Dies unterstreicht erneut die Bedeutung der physischen Elemente in der digitalen Welt.

Ein gezielter Ansatz ist die Erstellung von **User-Profilen**. Im März 2012 hat Google bekanntgegeben, dass Profile durch Verknüpfungen von Suchmaschinenutzungen, *YouTube, Google plus* und *gmail* erstellt werden[56]. Ähnliche Prozeduren sind auch von Betreiberfirmen sozialer Netzwerke bekannt, aber *Google* und andere Firmen wurden 2013 von einem mutmaßlich chinesischen Hackerangriff betroffen, bei dem Profile chinesischer Nutzer geprüft und exportiert wurden[57].

Hack the hackers: Wenn die Angreifer identifiziert sind, kann es sich lohnen, diese ihrerseits zu infiltrieren, um mehr über ihre Arbeitsweise zu erfahren.

Reales Praxisbeispiel: Die *New York Times* berichtete, dass die NSA in der Lage gewesen sei, in nordkoreanische Netzwerke über Malaysia und Südkorea vorzudringen, so dass sie in der Lage gewesen sei, nordkoreanische Hackeraktivitäten zu beobachten und nachzuverfolgen, aber eine offizielle Bestätigung dieser Darstellung wurde nicht gegeben[58].

Im Jahr 2017 wurde die Cyber-Sicherheitsfirma *Cellebrite* gehackt und Daten veröffentlicht. Diese zeigten, dass 40.000 lizenzierte Kunden (Nachrichtendienste, Grenzpolizei, Polizei, Militäreinheiten, Finanzorganisationen) z.B. das *Universal Forensic Extraction Device UFED* nutzten, die den Zugriff auf Smartphones durch die Nutzung von Sicherheitslücken (Exploits) ermöglicht. Weitere Exploit-Sammlungen für iOS, Android und Blackberry wurden veröffentlicht[59].

3.4.2 Intelligence Cooperation

Die Berichterstattung in den Medien vermittelte zuweilen den Eindruck, dass sich die nachrichtendienstliche Kooperation auf Computer und die Erfassung und Auswertung von allen Arten von Telekommunikation (**Signals Intelligence SigInt**) konzentriert. Die Zusammenarbeit wurde jedoch während des zweiten

[55] vgl. Schlüter/Laube 2010, S.8
[56] vgl. Spiegel 2013, S.111
[57] vgl. Süddeutsche Online 2013
58 vgl. FAZ 2015, S.5
59 vgl. Kurz 2017, S.13

Weltkrieges begonnen und dann im Zuge des kalten Krieges und der Terrorbekämpfung, die schon Jahrzehnte vor den Anschlägen des 11. September 2001 (9/11) begann, erweitert. Deshalb umfasst die Zusammenarbeit auch die Bearbeitung von Informationen, die von und durch Menschen gewonnen wurden (**human intelligence HumInt**), der Auswertung von Bildern (**imaging intelligence ImInt**) und von frei zugänglichen Informationen (**open source intelligence OsInt**)[60].

Das System der nachrichtendienstlichen Zusammenarbeit besteht aus drei Ebenen, der Zusammenarbeit der Dienste innerhalb eines Landes (**intelligence community**), der weitverbreiteten bilateralen Zusammenarbeit und der multinationalen Zusammenarbeit. Viele Staaten haben mehrere Dienste, die äußere und innere sowie zivile und militärische Angelegenheiten abdecken. Es gibt nicht endende Diskussionen über die optimale Zahl und Größe von Diensten: ein einheitlicher Dienst mag zu schwer zu kontrollieren sein, außerdem wäre der Schaden im Falle einer Infiltration enorm, und schließlich kann auch die interne Kommunikation zu kompliziert sein, so dass ggf. auch zu späte Reaktionen und blinde Flecken in der Bedrohungsanalyse entstehen können. Kleinere Organisationen können Spezialisierungsvorteile aufweisen, sind aber mit dem Risiko überlappender Aktivitäten und Verantwortlichkeiten behaftet, zudem kann es zu Konkurrenzdenken und Kommunikationsdefiziten zwischen den Einrichtungen kommen. Die Standardlösung sind mehrere Dienste mit einer koordinierenden Ebene[61]. Die größte **Intelligence Community** befindet sich in den USA (1981 formal etabliert), die seit 2004 (als Reaktion auf 9/11) vom *Director of National Intelligence DNI* koordiniert wird, davon sind die 8 militärischen Dienste in der Dachorganisation *Defense Intelligence Agency DIA*[62] zusammengefasst.

Die zweite Ebene wird durch ein Geflecht von **bilateralen Kooperationen** gebildet, z.B. Deutschland verfügt über Kontakte zu mehr als 100 Staaten[63]. Je nach Intensität und Qualität der politischen Beziehungen kann es sogar offizielle Repräsentanten (Legalresidenturen) geben, daneben ist es durchaus üblich, als (mehr oder weniger geduldete) Alternative Nachrichtendienstmitarbeiter als diplomatisches Personal in Botschaften bzw. Konsulate zu entsenden. Dies ist notwendig, um beide Länder betreffende nachrichtendienstliche Vorgänge und Belange zu erkennen, zu besprechen und ggf. auch zu bereinigen.

Die höchste Ebene der Zusammenarbeit ist die **multilaterale Kooperation**, denn selbst der größte Dienst verfügt nicht über die personellen, technischen oder

[60] vgl. Best 2009
[61] vgl. Carmody 2005
[62] vgl. DNI Handbook 2006
[63] vgl. Daun 2009, S.72

finanziellen Ressourcen, um den Globus vollständig abzudecken. Kleinere Gruppen können einfacher zu einer vertieften Zusammenarbeit gelangen als größere. Die USA hatten bereits nach dem 2. Weltkrieg die inzwischen offiziell bestätigte **5-eyes**-Kooperation mit Großbritannien, Kanada, Australien und Neuseeland eingerichtet und als Reaktion auf 9/11 die (offiziell nicht bestätigte, sondern im November 2013 von der Zeitung *The Guardian* und anderen[64] berichteten) erweiterten Kooperationen **9-eyes** mit Dänemark, Frankreich, den Niederlanden und Norwegen und **14-eyes** mit Belgien, Italien, Spanien, Schweden und Deutschland.

In der Europäischen Union begann die Zusammenarbeit mit der Bildung kleiner Arbeitsgruppen zur Terrorismusbekämpfung in den Siebziger Jahren und wurde danach schrittweise ausgebaut. Das Situation Center **SitCen** (welches seit 2010 dem *Standing Committee on operational cooperation on internal security COSI* untersteht)[65] wertet die Informationen aus, die von Organisationen der Mitgliedsstaaten, Arbeitsgruppen zur Terrorbekämpfung usw. geliefert werden. [66] Afrika hat inzwischen die multinationale Kooperation *Committee of Intelligence and Security Services of Africa CISSA* als Teil der Afrikanischen Union eingerichtet.

3.4.3 Konventionelle Anwendung von Intelligence

Jüngste Ereignisse von 2016 veranschaulichen die Relevanz der konventionellen Spionage für die Zuordnung. Wie bereits erwähnt, waren die Spannungen zwischen Russland und den USA bereits im Gange, da die russische Sicherheitsfirma *Kaspersky* Sinkholing gegen die vermutlich US-amerikanische *Equation Group* eingesetzt hat[67], die ihrerseits *Kaspersky* mit der anspruchsvollen Spionage-Malware *Duqu 2.0* infiziert hat[68].

Im August 2016 gab eine bis dahin unbekannte Gruppe namens **Shadow Brokers** an, Cyberwaffen der *Equation Group* in ihrem Besitz zu haben und veröffentlichten Material. Die Medien spekulierten, dass dies eine symbolische Warnung Russlands gewesen sei wegen der Verdächtigungen im sogenannten **DNC-Hack** in den Medien, d.h. sie wollten zeigen, dass auch sie in der Lage sind, Spionageaktivitäten der anderen zu verfolgen und ggf. bei Bedarf zu zeigen[69].

---

[64] wie z.B. Shane 2013, S.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] vgl. Scheren 2009

[67] vgl. Kaspersky Lab 2015a, S.34-35. Unerwarteterweise wiesen frühe Versionen der *Equation Group*-Malware hartcodierte (fest verankerte) IP-Addressen in ihren Programmen auf.

[68] vgl. Kaspersky Lab 2015b

[69] vgl. Jones 2016

Die Analyse der öffentlichen Datei zeigte Software von 2013; die Experten vermuteten, dass das Material von einem von der Equation Group genutzten Command and Control-Server kopiert wurde, also kein 'NSA hack' oder ähnliches stattgefunden hat.
Später publizierten die *Shadow Brokers* auch noch eine IP-Adressenliste von Computern, die die *Equation Group* infiziert und genutzt haben soll.
In einem späteren Statement auf *Pastebin* und *Tumblr* – das laut eigener Angabe von den Hackern selbst stammte- erklärten diese, dass das Material von einem Vertragsmitarbeiter der Firma *RedSeal* nach einer Sicherheitsübung kopiert worden war[70]. Das Material schien jedenfalls echt zu sein und einige Dateinamen waren identisch zu denen, die *Edward Snowden* als NSA-Tools bezeichnet hatte, wie z.B. *Epicbanana, Buzzdirection, Egregiousblunder, Bananaglee, Jetplow* und *Extrabacon*[71].

In den USA haben 1,5 Million Personen eine Sicherheitsstufe für Cyberangelegenheiten, davon arbeiten 480.000 in privaten Firmen[72]. Vom ODNI (*Office of the Director of National Intelligence*, das die Geheimdienste der USA, die *Intelligence Community*, koordiniert) wurde berichtet, dass 70% des Geheimdienstbudgets in private Firmen fließen[73]. Es wurde auf der anderen Seite darauf verwiesen, dass die Zusammenarbeit mit Privatfirmen schon lange besteht[74] und es notwendig ist, Expertenwissen für den rapide wachsenden Cybersektor nutzen zu können.

Der **Michailow-Vorfall:** Ende August 2016 wurde ein erfolgreiches Eindringen in Onlinewahlsysteme von Illinois und Arizona berichtet, in Illinois wurden Daten von 200.000 Wählern kopiert[75]. Die Medien spekulierten darüber, dass dies Teil einer russischen Kampagne sei, definitive Beweise wurden bisher aber nicht gefunden.[76] Aber dann wurde festgestellt, dass eine Firma namens *King Server* sechs Server für diesen Angriff von einer Firma namens *Chronopay* mietete. Der russische Besitzer von *Chronopay* wurde bereits von *Sergej Michailow*, einem Mitglied der russischen Intelligence Cyber-Unit CIB des Nachrichtendienstes FSB untersucht, der (nach Berichten z.B. aus der Zeitung *Kommersant*) die US-Behörden über diese Angelegenheit informierte.[77]. *Russia Today* bestätigte, dass es einen Fall Michailow gibt, ohne die Einzelheiten des Informationslecks zu

[70] vgl. Ragan 2016
[71] vgl. Steier 2016, Spiegel online 2016, Solon 2016
[72] vgl. Gartmann/Jahn 2013, S.24
[73] vgl. Huber 2013, S.18-19
[74] *BAH* knackte die Codes deutscher U-Boote im zweiten Weltkrieg, vgl. Gartmann/Jahn 2013, S.24. Andere Sicherheitsfirmen sind z.B. *Xe* und *USIS*.
[75] vgl. Nakashima 2016, Winkler 2016, S.4
[76] vgl. Winkler 2016, S.4
[77] vgl. FAZ 2017, S.5

bestätigen und stellte klar, dass der Fall zusammen mit anderen Vorgängen noch von den russischen Behörden untersucht wird[78].

Der **Surkov-Vorfall**: Mitte Oktober 2016 gab US-Vizepräsident *Joe Biden* bekannt, dass die USA ernsthaft eine Cyber-Vergeltung gegen Russland aufgrund ihrer vermuteten Beteiligung am *DNC-Hack* und anderen Dingen erwägen würden[79]. Ein paar Tage später, d.h. noch vor den Präsidentenwahlen in den USA, präsentierte eine ukrainische Gruppe namens *CyberHunta* den Hack der E-Mail-Box des Büros des wichtigen russischen Präsidentenberaters *Vladislav Surkov*. Zumindest Teile des Materials konnten als echt verifiziert werden, d.h. als nicht fabriziert. Allerdings bezweifelten US-Medien, dass eine solche Top-Level-Operation von einer ukrainischen Gruppe ohne eine entsprechende Hacking-Vorgeschichte durchgeführt werden könnte, sondern dass dies stattdessen eine Warnung der US-Nachrichtendienste war[80].

Der *US Intelligence Community Report on Cyber incident Attribution* von 2017, der im Einklang mit der vorherigen Bewertung der Operationen von *APT28/Fancy Bears* und *APT29/Cozy Bears* als Operation *Grizzly Steppe* stand, betonte stark die politische Motivation von Russland als Argument für die Zuordnung der Angriffe zu Russland[81].
Dies wurde in den Medien als begrenzte Beweislage kritisiert, aber die Vorfälle mit *Michailow* und *Surkov* deuten darauf hin, dass sich möglicherweise mehr hinter den Kulissen abspielte als nur eine digitale Zuordnung und Analyse politischer Motivationen.

4. Attribution im Cyberwar

Der Begriff **Cyberwar** (auch: cyber war, cyber warfare, Cyber-Krieg, Krieg der Computer, Computerkrieg) ist aus den Begriffen War und Cyberspace

[78] vgl. Russia Today (RT Deutsch) online 27.01.2017
[79] vgl. Zeit online 2016
[80] vgl. Shuster 2016
[81] ODNI 2017, JAR 2016 des *Department of Homeland Security DHS* und des *Federal Bureau of Investigation FBI*. *APT 28/Fancy Bears* und *APT29/Cozy Bears* richten sich auf Ziele mit politischer Relevanz für Russland. Die Zeitzonen für die Kompilierung der Malware decken sich mit der Moskauer Standardzeit, die russische Sprache wird verwendet und typischerweise werden Tools für langfristige Einsätze angewendet. Die eingebauten Hintertüren nutzen das http-Protokoll und den Mailserver des Zielcomputers, vgl. Weedon 2015. *APT 28* nutzt eine Vielfalt an Malware *(Sofacy, X-Agent, X-Tunnel, WinIDS, Foozer* und *DownRange)* und verfügt auch über Malware für Smartphones, vgl. Alperovitch 2016. The Dukes sind eine Malwarefamilie mit einer stetig wachsenden Zahl an Werkzeugen wie *MiniDuke, CosmicDuke, OnionDuke, CozyDuke, CloudDuke, SeaDuke, HammerDuke, PinchDuke und GeminiDuke*, die von *APT29/Cozy Bears* genutzt werden, vgl. Weedon 2015. Die Attacken zeigen ein zweistufiges Vorgehen mit einem initialen Einbruch in das attackierte System, dem, falls es sich um ein relevantes Ziel handelt, der Übergang zu einer Langzeitüberwachung folgt, vgl. F-Secure Labs 2015. Für dieses Vorgehen sind mehrstufige Ladevorgänge und Backdoors verfügbar. Um eine Entdeckung zu verhindern, prüft die Malware die Sicherheitseinstellungen des Computers sehr gründlich.

zusammengesetzt und bezeichnet die kriegerische Auseinandersetzung mit den Mitteln der Informationstechnologie.
Die Zuordnung im Cyberkrieg ist aus der theoretischen und rechtlichen Perspektive das wichtigste Attributionsproblem, da die Frage "*Wer war es?*" zur Vergeltung oder gar Krieg führen kann, wenn ein bestimmtes Schadensausmaß überschritten wird. Allerdings ist die praktische Relevanz der Sache fraglich, da es ein **Attributions-Paradoxon** gibt.

Zunächst einmal stimmten die Cyber-Kriegs-Konzepte von US und China von Anfang an dahingehend überein, dass der Einsatz von Computern im militärischen Bereich nur ein Teil anderer militärischer Aktivitäten ist. Die Debatte über die Frage, ob ein Krieg durch Computerangriffe allein entschieden werden kann, ist rein theoretischer Natur, für die militärische Praxis wurde diese Option niemals in Betracht gezogen.

Manchmal wird auch diskutiert, ob Computer wirklich ein Teil eines Krieges sein könnten, da Computerangriffe Menschen nicht töten konnten, aber in der militärischen Praxis ist diese Debatte irreführend. Computer sind einfach technische Werkzeuge wie z.B. Radarsysteme. Radarsysteme töten die Feinde nicht direkt und in der Tat retten sie viele Leben im zivilen Luftverkehr, aber niemand würde daran zweifeln, dass Radarsysteme auch ein Teil anderer militärischer Aktivitäten sind.

General Keith Alexander, der ehemalige Chef des Cyber Command CYBERCOM und der NSA legte seine Vorstellungen zum Cyberwar bereits 2007 dar und beschriebe diesen als integralen und *unterstützenden* Bestandteil allgemeiner militärischer Operationen und dass dieser nicht nur offensive, sondern auch defensive Komponenten enthält[82]. Das bedeutet aber auch, dass der Cyberwar ein Zusammenspiel von Mensch und Maschine ist, also die Computer dies nicht alleine durchführen können und dass es sich in Anpassung an die jeweilige Lage um ein ganzes Bündel von Maßnahmen handelt, also in der Regel nicht nur um einen einzigen Schlag geht, auch wenn ein solcher am Anfang stehen mag.

Das Primärziel aller Akteure ist die Erringung der **elektromagnetischen Dominanz** und insbesondere der **Überlegenheit im Cyberspace**[83], d.h. der Beherrschung des Cyberspace im Konfliktfall. Da die gegnerischen Systeme jedoch wiederhergestellt werden können, beschränkt sich die Zielsetzung in der Praxis auf die Sicherstellung der eigenen Handlungsfreiheit (**freedom of action**) und die Beschränkung der Handlungsfreiheit des Feindes, wobei beides im Verbund mit konventionellen Operationen steht.

[82] vgl. Alexander 2007, S.60
[83] vgl. USAF 2010, S.2

Die chinesische Strategie besteht darin, zunächst das gegnerische Netzwerk zu treffen, um dann die resultierende ‚**operative Blindheit**' des Gegners mit konventionellen Waffen zu überprüfen und ggf. weiter vorzugehen[84]. Natürlich besteht das Risiko, dass der Gegner sein Netz wieder repariert, so dass diese Strategie auf lange Sicht erfolglos sein kann; um so wichtiger ist es, in der Frühphase des Konflikts die Oberhand zu gewinnen und die „**elektromagnetische Dominanz**" so lange wie möglich zu behalten. Die Strategie ist natürlich riskant, falls sich der Gegner unerwartet schnell regeneriert oder nicht im gewünschten Ausmaß getroffen werden kann. US-Studien zeigen, dass sich ein solcher Krieg wohl nur über einen sehr begrenzten Zeitraum wirksam führen lässt. [85]

Die US- und chinesischen Cyberwar-Konzepte zeigen deutlich, dass ein konventioneller Schlag gleichzeitig oder sehr kurz nach dem Cyber-Angriff durchgeführt werden muss, wenn die militärische Aktion erfolgreich sein soll. Dies bedeutet, dass die Zuordnung des Cyber-Angriffs innerhalb von Minuten möglich ist, weil der Zielstaat gleichzeitig dem feindlichen Feuer ausgesetzt sein wird, d.h. der Angreifer *identifiziert sich selbst*.

Reales Praxisbeispiel: Bei dem Angriff auf eine mutmaßliche Atomanlage in Ostsyrien am 06.09.2007 mussten israelische Flugzeuge den gesamten syrischen Luftraum durchfliegen. Um dies zu ermöglichen, hatten die Israelis den Computern der syrischen Luftabwehr einen leeren Himmel vorgegaukelt, so dass die Flugzeuge unbehelligt einfliegen und angreifen konnten. Dies ist ein klassisches Beispiel für die Idee des Cyberwars als operativer Ergänzung zu konventionellen Maßnahmen[86].

Wenn ein massiver Cyber-Angriff ohne einen konventionellen Schlag durchgeführt wird, hat der Zielstaat Zeit, die Systeme zuerst wiederherzustellen und die Attribution in der Zwischenzeit zu beginnen, die mit aggressivem Gebrauch von nachrichtendienstlichen Methoden weniger Zeit in Anspruch nehmen kann, als die Angreifer erwarten.
Auf der anderen Seite ergibt sich eine Art **reverse attribution**, d.h., von der physischen zur digitalen Welt. In der Ära der Spionage-Satelliten wird die Vorbereitung eines großen Militärschlags nicht unentdeckt bleiben und er kommt typischerweise nach massiven politischen Spannungen, d.h. es gibt klare Warnzeichen in der physischen Welt für Angriffe in der digitalen Welt.

[84] vgl. Krekel et al. 2009
[85] vgl. Tinner et al. 2002
[86] vgl. Herwig 2010, S.60

5. Abschließende Bemerkungen

Das Papier hat gezeigt, dass Attribution ein cyber-physischer Prozess ist, der die digitale und die physische Welt umfasst.

Die Attributionsbemühungen haben in den letzten Jahren erhebliche Fortschritte gemacht und es können weitere rasche Fortschritte erwartet werden. Allerdings werden die Angreifer wohl immer einen Schritt voraus sein, denn Hacker werden weiterhin neue Schwachstellen finden und bisher unerwartete Möglichkeiten, Computer und Geräte anzugreifen.

Attribution ist nicht nur das Sammeln von Informationen, sondern auch die Interpretation und Kombination von Fakten. Die Attributionsdiskussion ist oft kontrovers und so muss jede abweichende Theorie überprüft werden, ob sie neue Fakten oder bessere Interpretationen der vorhandenen Erkenntnisse präsentiert.

Die Zusammenarbeit zwischen Organisationen durch Kombination von Ressourcen, Erfahrung und Wissen ist ein Schlüsselelement des zukünftigen Erfolgs der Attribution von Cyberattacken.

6. Literaturquellen

Abendzeitung (2014): USA halten einige Lücken in Computersystemen geheim. Abendzeitung online 29.04.2014

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

Alperovitch, D. (2014): Deep in Thought: Chinese Targeting of National Security Think Tanks 07.07.2014, 8 S.

Alperovitch, D. (2016): Bears in the Midst: Intrusion into the Democratic National Committee. From The Front Line, update 15.06.2016, 3 S.

Alvarez, S., Jansen, F. (2016): Hackerangriff auf die Telekom. Der Tagesspiegel online 28.11.2016

Baches, Z. (2016): Wie Hacker eine Notenbank knacken. Neue Zürcher Zeitung, 10.10.2016, S.7

Baumgärtner, M., Neef, C. Stark, H. (2016): Angriff der Bären. Der Spiegel 31/2016, S.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, S.126 ff.

Brächer, M. (2016): Das fragile Netzwerk. Handelsblatt Nr. 155/2016, S.26-27

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

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, S.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, S.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. FAZ Nr. 136, 15.06.2013, S.1

FAZ (2015): “NSA hat Computer in Nord-Korea schon vor 4 Jahren infiltriert”. Frankfurter Allgemeine Zeitung, 20.01.2015, S.5

FAZ online (2015): Cyber-Angriff auf TV5 Monde. Ermittler verfolgen Spur nach Russland. FAZ online 09.06.2015

FAZ (2017): Geheimdienstler verhaftet. Frankfurter Allgemeine Zeitung, 28.01.2017, S.5

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

Fuest, B. (2014a): Uroburos –Russisches Supervirus greift die Welt an. Welt am Sonntag online 10.03.2014, 3 Seiten

Fuest, B. (2014b): Der übliche Verdächtige. Welt Am Sonntag Nr. 52/2014

Gartmann, F., Jahn, T. (2013): Die Geheim-Dienstleister. Handelsblatt 26.06.2013, S.24

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

Glenny, M. (2010): Die neuen Cyberkrieger. Financial Times Deutschland, 12.10.2010, S.23/26

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

Gutscher, Th. (2013): Menschenrechte hochhalten, nach Daten tauchen. Frankfurter Allgemeine Sonntagszeitung Nr.26 30.06.2013, S.7

Herwig, M. (2010): Die @-Bombe. Welt Am Sonntag Nr.39, 29.06.2010. S.60-61

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

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

Jennifer (2014): Breaking the Code on Russian Malware. The Recorded Future Blog Posted in Cyber Threat Intelligence 20.11.2014

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? 19.08.2016 Financial Times online, 7 S.

Kaspersky (2013): “Winnti” Just more than a game. April 2013, 80 S. und Appendix

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

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

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

Kaspersky Lab (2015c): Der große Bankraub: Cybergang “Carbanak” stiehlt eine Milliarde US-Dollar von 100 Finanzinstituten weltweit, Moskau/Ingolstadt, 15.02.2015, 3 Seiten

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

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 20.02.2017

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 Nr. 31, 06.02.2017, S.13

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

Mayer-Kuckuck, F., Koenen, J., Metzger, S. (2012): Hacker werden immer dreister. Handelsblatt 15.02.2012, S.20-21

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

Müller, G.V. (2016): Der Verpächter des Internets. Neue Zürcher Zeitung, 01.11.2016, S.7

Nakashima, E. (2016): Russian hackers targeted Arizona election system. 29.08.2016. Washington Post online, 29.08.16, 4 S.

Novetta (2015): Operation-SMN-Report Juni 2015, 31 Seiten

Novetta (2016): Operation-Blockbuster-Report Februar 2016, 59 Seiten

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 Seiten

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

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

Russia Today (RT Deutsch) online (2017): Russland: FSB und Kaspersky Lab in Erklärungsnot – Landesverrat im Bereich Cybersicherheit vermutet. 27.01.2017

Sanger, D.E. (2015): US and China seek arms deal for cyberspace. New York Times online 20.09.2015, 5 S.

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

Schlüter, N., Laube, H. (2010): Der RIM-Code. Financial Times Deutschland 03.08.2010, S.8

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

Shuster, S. (2016): Hacker Kremlin Emails could signal a turn in the U.S.-Russia Cyberwar. Time Magazine online 07.11.2016

Solon, O. (2016): Hacking group auctions 'cyber weapons' stolen from NSA. The Guardian online, 16.08.2016, 2 S.

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

Spiegel online (2016): Gruppe "Shadow Brokers" Hacker erbeuteten offenbar NSA-Software. 17.08.2016, 1 S.

Steier, H. (2016): Riskantes Horten von Sicherheitslücken. Neue Zürcher Zeitung online, 18.08.2016, 2 Seiten

Storn, A. (2016): Plötzlich sind 81 Millionen Dollar weg, Die Zeibt Nr.20, 04.05.2016, S.29

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

Symantec (2016a): The Waterbug attack group. Security Response Version 1.02 Symantec, 14.01.2016, 44 Seiten

Symantec (2016b): Strider: Cyberespionage group turns eye of Sauron on targets, Symantec Official Blog, 07.08.2016

Symantec (2016c): Odinaff: New Trojan used in high level financial attacks, Symantec Official Blog, 11.10.2016

SZ online (2013): Fernseher schaut zurück. Artikel vom 21.11.2013

Tellenbach, B. (2017): Darknet macht keine neuen Kriminellen. Neue Zürcher Zeitung 17.02.2017, S.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, S.228-23

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

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, S.67-77

Wehner, M. (2015): Cyber-Krieg im Bundestag. Frankfurter Allgemeine SonntagsZeitung Nr.24 vom 14.06.2015, S.1

Welchering, P. (2013): Mit Vierkantschlüssel und Biege-Koppler. Frankfurter Allgemeine Zeitung Nr. 156/2013, S.6

Welchering, P. (2014): Arbeiten am Trojaner-Abwehrschirm. Frankfurter Allgemeine Zeitung vom 09.09.2014, S.T4

Welchering, P. (2016): So fahndet der Geheimdienst NSA nach Programmierern. Frankfurter Allgemeine Zeitung Nr. 136/2016, S.T4

Winkler, P. (2016): Russische Hacker in Amerikas Wahlregistern. Neue Zürcher Zeitung, 01.09.2016, S.4

Wittmann, J. (2017): Gesucht: Bond. Jane Bond. Neue Westfälische 11.02.2017

Zeit online (2016): Mögliche CyberAttacke soll Russland bloßstellen. Oktober 2016, 2 S.

Zepelin, J. (2012): Länder lahmlegen. Financial Times Deutschland 06.07.2012, S.27