Thomas Reinhold - cyberpeace.org
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

Von den Realitäten im Cyberwar - oder -
Die Bedeutung des Sony-Hack für zukünftige Cyber-Konflikte

Ende November des vergangenen Jahres wurde das US-amerikanische Unternehmen Sony Pictures Entertainment (SPE) Opfer einer groß angelegten Hackerkampagne. Dabei wurden Daten von Angestellten und Kooperationspartnern, wie Namen, Adress- und Versicherungsangaben aber auch Finanzinformationen und Verschlüsselungsdaten[1] entwendet und viele Arbeitsplatzrechner des SPE-Netzwerkes durch eine Schadsoftware infiziert. Aussagen hochrangiger Sony-Mitarbeiter[2] zufolge wollten die Angreifer Sony mit den erbeuteten Daten ursprünglich um Geld erpressen. Medial wurde der Vorfall jedoch rasch mit der anstehende Premiere der von SPE produzierten Komödie "The Interview"[3], die sich satirisch mit der Situation in Nordkorea auseinandersetzt, in Verbindung gesetzt. Jedoch trat erst Mitte Dezember eine Hackergruppe names "Guardians of Peace" mit Forderungen gegen die Ausstrahlung des Films als Urheber der Hacking-Attacke auf und drohte mit der Veröffentlichung der entwendeten Sony-Daten[4]. Kurz darauf wurde der Sony-Hack auch durch das FBI offiziell bestätigt und staatliche Einrichtung Nordkoreas als Urheber der Angriffe beschuldigt[5]. In der Beweisführung bezog sich das FBI auf Erkenntnisse und Ähnlichkeiten zu früheren Vorkommnisse in den USA und Süd-Korea sowie den geografischen Standorten der IP-Adressen einiger, für den Angriff benutzen Computer[6]. Obwohl das FBI in seiner Meldung von Angriffen zerstörender ("destructive") Natur spricht, gibt es gegenwärtig keine verlässlichen Informationen über tatsächliche Schäden die durch die Hackerattacke entstanden sind und auch die Aussagekraft der offiziellen FBI-Belege werden durch IT-Sicherheitsexperten eher angezweifelt:

In general, it's a situation that rapidly devolves into storytelling, where analysts pick bits and pieces of the "evidence" to suit the narrative they already have worked out in their heads (Bruce Schneier)[7].

Vor dem Hintergrund eines kurzzeitigen Veröffentlichungsstops des Films durch SPE und mit Verweis auf die FBI-Erkentnisse wurden seitens der US-Regierung trotz der Zweifel "angemessene Reaktionen"[8] gegenüber Nordkorea angedroht. Da man die Vorfälle als kritische Cyber-Attacken wertete, wurden Anfang des neuen Jahres Strafmaßnahmen wie Handels- und Reisebeschränkungen gegen staatliche Einrichtungen, Unternehmen und Einzelpersonen Nordkoreas verhängt[9]. Die geschilderten Vorfälle rund um die Hacking-Attacke gegen das Sony-Netzwerk, jedoch insbesondere die ungewöhnliche schnelle Reaktion und die Bestimmtheit in der Frage des Angreifers werfen jedoch einige Fragen auf – vor allem gemessen an früheren Vorfällen wie sie bspw. im Madiant-Report[10] ausgewertet wurden. Dieses Verhalten der US-Regierung demonstriert darüber hinaus welche Rolle dem Cyberspace in zwischenstaatlichen Konflikten zukünftig möglicherweise zukommt und wie diese Konflikte ausgetragen werden könnten.

---

1 http://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf
2 http://www.bloomberg.com/news/2014-11-24/sony-corp-computers-said-hacked-in-possible-blackmail.html
3 http://de.wikipedia.org/wiki/The_Interview
4 https://www.tagesschau.de/wirtschaft/sony-hack-101.html
5 http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
6 http://www.golem.de/news/guardians-of-peace-sony-hack-wird-zum-politikum-1412-111280.html
7 https://www.schneier.com/blog/archives/2014/12/did_north_korea.html
8 http://www.nytimes.com/2014/12/20/world/fbi-accuses-north-korean-government-in-cyberattack-on-sony-pictures.html
9 http://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx
10 http://intelreport.mandiant.com/

Dies betrifft zum einen die Beweisführung des FBI und der US-Regierung. Aus Sicht eines Informatikers schließe ich mich den kritischen Betrachtungen und Zweifeln meiner Kollegen an[11]. Schadsoftware wird nach deren Bekanntwerden oft vielfach kopiert, durch Dritte weiterverwendet oder für eigene Zwecke angepasst. Ähnlichkeiten in der Form der verwendeten Schadsoftware oder die verwendete Sprache von Text-Bausteinen innerhalb des Programmcodes können bei der Entwicklung der Software rasch zustande kommen oder auch bewusst als falsche Fährte eingebaut werden. Die FBI-Aussagen enthalten auch keine Hinweise auf die Qualität der Schadsoftware und der eingesetzten Angriffsmethoden. Dies legt den Schluss nahe, dass der Angriff eher mit Hilfsmitteln durchgeführt wurde, die weit verbreitet sind und sich nicht durch besonders hoch-entwickelte Methoden hervorheben. Ein weiterer zweifelhafter Aspekt in der US-amerikanischen Argumentation betrifft die Aussagekraft der geographischen Zuordnung von IP-Adressen. Eine detaillierte Analyse sämtlicher bekannter Adressen eines Sicherheits-Spezialisten[12] kam dabei zu folgenden Schluss:

Drei davon führen zu Servern in Thailand, Polen und Italien. Vier weitere hat er in Bolivien, Singapur und sogar in den USA entdeckt. Allesamt haben sie eines gemeinsam: Sie sind dafür bekannt, Malware und Spam zu verbreiten und sind möglicherweise selbst kompromittiert worden.[13]

Insbesondere der Aspekt der geographischen Verortung von IP-Adressen und die Identifikation eines Angreifers wurde seit Stuxnet international umfassend diskutiert. Diese sogenannte Attribution ist unter anderem für völkerrechtlich legitimierte Reaktionen auf Angriffe, wie dem Recht auf Selbstverteidigung nach UN Charta Art. 51[14], eine zwingende Voraussetzung. Dabei sind die genannten Schwierigkeiten im Falle des Sony-Hacks keineswegs herausragend sondern systemisch bedingt durch die Funktionsweise des Cyberspace. Da Hacking-Angriffe in aller Regel über solche zwischengeschalteten Computersysteme durchgeführt werden, ist es bei konkreten Vorfällen aufgrund dieser Möglichkeiten Spuren im Netz zu verschleiern zusätzlich schwer nachzuweisen, ob hinter einem Angriff staatliche Einrichtungen - wie im Falle des Sony-Hacks möglicherweise die “Bureau 121”[15] genannte Hacking-Einheit Nordkoreas oder sub-nationale Gruppen ohne staatlichen Auftrag oder staatliche Kontrolle stehen. Aufgrund dieser Schwierigkeiten wurde die geringe Beweiskraft von IP-Adressen und eine darauf beruhende Attribution bisher als eine der größten Schwierigkeiten bei der Übertragung völkerrechtlicher Normen auf den Cyberspace angesehen:

Even if constructive knowledge suffices, the threshold of due care is uncertain in the cyber context because of such factors as the difficulty of attribution, the challenges of correlating separate sets of events as part of a coordinated and distributed attack on one or more targets, and the ease with which deception can be mounted through cyber infrastructure.
(Tallin Manual on the international Law applicable to cyber warfare[16])

Vor diesem Hintergrund überrascht es, mit welcher Schnelligkeit, und Bestimmtheit im aktuellen Fall die USA Nordkorea als Angreifer beschuldigt und Sanktionen verhängt haben. Einerseits kann dies darauf hindeuten, dass den zuständigen Behörden mehr Informationen zur Verfügung stehen, als öffentlich verlautbart wurde. Mit Blick auf die Enthüllungen aus den Snowden-Fundus und den Überwachungsmöglichkeiten der NSA kann dies als wahrscheinlich angesehen werden, insbesondere da die NSA laut aktuellen Veröffentlichungen[17] seit 2010 Nordkoreanische

---

[11] https://www.schneier.com/blog/archives/2014/12/did_north_korea.html
[12] https://krypt3ia.wordpress.com/2014/12/20/fauxtribution/
[13] http://www.golem.de/news/sony-hack-die-dubiose-ip-spur-nach-nordkorea-1412-111314.html
[14] http://www.un.org/en/documents/charter/chapter7.shtml
[15] http://www.bloomberg.com/news/2014-12-07/sony-s-darkseoul-breach-stretched-from-thai-hotel-to-hollywood.html
[16] http://www.cambridge.org/us/academic/subjects/law/humanitarian-law/tallinn-manual-international-law-applicable-cyber-warfare
[17] http://heise.de/-2519669

Computernetze infiltriert haben soll. Andererseits kann das Verhalten auch vor dem Hintergrund der jüngsten US-Verteidigungsdoktrin interpretiert werden, die explizit offensive Cyber-Attacken als Möglichkeiten zur Wahrung der nationalen Sicherheit und der militärischen Hoheit der USA vorsieht und Bedrohungen durch den Cyberspace in den Kanon der nationalen Sicherheitsarchitektur aufnimmt:

OCO ["Offensive Cyberspace Operations", Anm. des Redakteurs] are CO ["Cyberspace Operations", Anm. des Redakteurs] intended to project power by the application of force in and through cyberspace. OCO will be authorized like offensive operations in the physical domains, via an execute order (EXORD) [..] Cyberspace Attack ["are"] cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. (Joint Publication 3-12 (R) - Cyberspace Operations - Doctrine on strategic and offensive military cyber operations[18])

Die rasche und zielgerichtete Reaktion könnte daher auch primär auf politische Gründe zurückzuführen sein und als Signal verstanden werden, auf derartige Cyber-Bedrohungen zukünftig zeitnah und mit offensiv wirksamen Mitteln zu reagieren, ohne sich dabei zu sehr durch diffizile Fragen der Attribution, die lange als "Versteck der Cyber-Bösen" angesehen wurden, aufhalten zu lassen. Insbesondere unter dem Gesichtspunkt einer Abschreckung potentieller Gegner durch militärische Cyber-Arsenale wäre ein solches Signal schlüssig um die Wirksamkeit der Verteigigungspotentiale zu demonstrieren.

"(..) From a diplomatic perspective, it's a smart strategy for the US to be overconfident in assigning blame for the cyberattacks. Beyond the politics of this particular attack, the long-term US interest is to discourage other nations from engaging in similar behavior. If the North Korean government continues denying its involvement, no matter what the truth is, and the real attackers have gone underground, then the US decision to claim omnipotent powers of attribution serves as a warning to others that they will get caught if they try something like this", Allan Friedman, a research scientist at George Washington University's Cyber Security Policy Research Institute.[19]

In diese Deutungsversion der Geschehnisse passen auch Cyber-Attacken auf nord-koreanische IT-Netze kurz vor Weihnachten 2014, bei der große Teile das Land für zehn Stunden vom Rest des Internets getrennt wurden. Unabhängig davon, ob diese Angriffe tatsächlich durch staatliche Einrichtungen der USA durchgeführt wurden - was von Experten angezweifelt wird[20] - ist bezeichnend, dass die stellvertretende Sprecherin des US-Außenministeriums, Marie Harf, sich auf die Frage nicht äußern wollte, ob die USA für den Ausfall des nordkoreanischen Netzes verantwortlich seien[21].

Grundsätzlich war und ist die Frage nach der Herkunft und die Bewertung eines Angriffs aus Sicht des angegriffenen Staates in klassischen Konflikten neben einer juristisch stichhaltigen Argumentation stets auch eine Frage des weltpolitischen Zeitgeistes und der nationalen Interessen. Angesichts der im Cyberspace zusätzlich erschwerten Herkunftsortung von Angriffen überrascht der vorliegende Fall gerade aufgrund des Mangels an forensischen Beweisen durch seinen Verlauf und den zu vermutenden im Vordergrund stehenden politischen Interessen. Damit könnte der Fall Hinweise darauf liefern, wie der Cyberspace zukünftig Gegenstand oder Austragungsort zwischen-staatlicher Konflikte sein kann oder wie Staaten sicherheits- und außenpolitische Interessen und Ziele auch durch Aktivitäten im Cyberspace umzusetzen versuchen. Damit würde

---

[18] http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf
[19] https://www.schneier.com/blog/archives/2014/12/did_north_korea.html
[20] http://threatpost.com/u-s-sanctions-north-korea-defense-agencies-individuals-in-sony-hack/110182
[21] http://www.zeit.de/politik/2014-12/nordkorea-sicherheitsrat-menschenrechte

das politische Alltagsgeschäft faktisch an den bisher eher akademisch geführten Debatten, wie der Entwicklung einer Klassifikation von Cyberwaffen und Cyberattacken oder der Übertragung etablierter Normen des Völkerrechts auf den Cyberspace ”vorbeiziehen” und mit der normativen Kraft des Faktischen die Zukunft der militärischen Nutzung dieser weltweiten Domäne bestimmen.