Timing of Cyber Conflict

Fabian Heidler
Betreuer: Heiko Niedermayer
Seminar Future Internet WS2014
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: ga46zuy@in.tum.de

Diese Arbeit soll darüber Einblick geben wann der richtige Zeitpunkt gekommen ist, eine Lücke in einem fremden Sicherheitssystem auszunutzen. Dazu wird ein grundlegendes mathematisches Modell erklärt und anschließend an einigen Beispielen demonstriert. Des Weiteren soll die Bedeutung von Cyber Conflict erkannt werden, und Ausblick gegeben werden welche Rolle dieser in der Zukunft einnimmt. Abschließend wird noch eine mögliche Anwendung in Computerspielen diskutiert.

1. Einleitung

1.1 Was ist Cyber Conflict

Cyber Conflict ist das Nutzen von Computer Ressourcen um Informationen zu beschaffen oder Schaden zu verursachen. Die Ressourcen die Staaten oder Organisationen hier ansammeln werden Exploits genannt. Dies ist eine Möglichkeit eine Schwachstelle in einem System auszunutzen, die bei der Implementierung übersehen wurde. Dies ist nicht zu verwechseln mit der Vulnerabilität, welche die Sicherheitslücke darstellt. Exploits werden sowohl zum Diebstahl von Daten genutzt, aber auch zur simplen Sabotage an Hardware . Ein Zero – Day – Exploit beschreibt einen möglichen Angriff auf eine Schwachstelle, der bereits sehr kurz nach Release der Software entwickelt wurde und folglich in dieser Form noch nicht bekannt ist. Wird diese Schwachstelle nicht direkt von den Entwicklern selbst entdeckt, besteht die Möglichkeit dass diese lange unentdeckt bleibt. Das macht Zero – Day – Exploits so wertvoll. Der Direktor der National Security Amerikas, nannte Cyber Security als wichtigste Bedrohung der sich Amerika gegenüber sieht. Nachdem immer mehr Systeme sich ausschließlich auf Software verlassen, wird also auch die Bedeutung von Cyberkrieg wichtiger. Der Schaden der hierbei entstehen kann lässt sich in 6 Felder einteilen:

- Verlust von geistigem Wissen und vertraulichen Informationen
- Cyberkriminalität,
- Diebstahl von vertraulichen Geschäftsinformationen und damit die eventuelle Manipulation von Börsendaten
- Kosten für die Verteidigung der Netzwerke sowie Versicherungskosten
- Rufmord an betroffenen Firmen[1]
- Opportunitätskosten

Anzumerken ist noch, dass ein wirksamer Angriff häufig nicht nur aus einem Exploit besteht. Eine sinnvolle Ressource, kann also mehrere Exploits beinhalten und greift eventuell auch auf nicht technische Hilfsmittel zurück, zum Beispiel einen Insider, der den Angriff einschleust.

1.2 Ablauf eines Exploits

Den Anfang macht immer das unabsichtliche Einschleusen eines Bugs in das Programm. Das Programm wird also mit Schwachstellen an die Verbraucher gebracht. Irgendwann wird die Schwachstelle entdeckt, und ein Exploit wird entwickelt um diese auszunutzen, meistens von Kräften aus der Unterwelt. Nach dem - für eine gewissen Zeitspanne - heimlichem Einsatz, also der Zero – Day - Attack, erfährt der Entwickler von der Lücke, entweder durch Tests oder durch Meldungen von Nutzern, und beginnt an einem Patch zur Behebung zu arbeiten. Kurz darauf wird die Vulnerabilität an die Öffentlichkeit weitergegeben, was zu Follow – on – attacks führt. Dadurch wissen nun auch Anti-Virus Hersteller von der Lücke und updaten ihre Programme um diese zu erkennen. Endnutzer mit aktuellem Anti-Viren Programm können nun erkennen, ob sie infiziert sind. Kurz nach Veröffentlichung durch den Hersteller, wird der Patch freigegeben und die Nutzer der aktuellen Version sind wieder geschützt (siehe auch Bild 1).

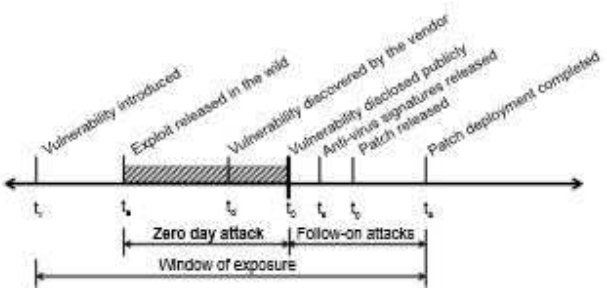

Bild 1. Zeitlicher Ablauf eines Zero – Day – Exploits [2]

In dieser Arbeit soll nun ein Model von Robert Axelrod und Rumen Iliev näher gebracht werden, welches sich damit auseinandersetzt, wann der Zeitpunkt gekommen ist, einen Zero – Day – Exploit einzusetzen. Das Schwierige dabei ist abzuschätzen, ob es sich bereits lohnt seinen Exploit zu zeigen, wobei dieser dann möglicherweise nicht mehr einsetzbar ist. Auf der anderen Seite kann zu langes Warten dazu führen dass die Schwachstelle entdeckt wird und der Exploit nutzlos geworden ist. Da dieses Model sehr mathematisch ist, werden zum besseren Verständnis drei Ereignisse gezeigt: der iranische Angriff auf Saudi Aramco, die tägliche Cyber Spionage Chinas und ein frühzeitiger Einsatz Chinas gegen Japan.

doi: 10.2313/NET-2015-03-1_03

2. Mathematisches Modell

2.1 Erklärung

2.1.1 Der Einsatz

Die erste Variable die zu berücksichtigen ist, stellt der Einsatz dar. Oder in anderen Worten: Wie viel steht zum derzeitigen Zeitpunkt auf dem Spiel. Das Problem hierbei ist, dass zwar bekannt ist was im Moment der Einsatz ist, jedoch lässt sich keine Aussage darüber treffen wie sich dieser entwickelt. In Kriegszeiten hat eine Ressource also einen deutlich höheren Wert, als wenn Frieden herrscht. Doch auch ohne Konflikt kann ein Land Interesse haben an der Technologie eines anderen. Dann würde der Einsatz auf einem mittleren Level stehen. Insgesamt ist der Einsatz durch die gesamte Vernetzung der Welt und unvorhersehbaren politischen Ereignissen am schwersten einzuschätzen.

2.1.2 Stealth und Persistence

Das Überleben einer Ressource hängt maßgeblich von 2 Faktoren ab. Zum einen von ihrer Tarnung („Stealth) und zum anderen von ihrer Beständigkeit („Persistence“). Stealth gibt dabei an, wie hoch die Wahrscheinlichkeit ist, dass nach Benutzung der Ressource, sie unentdeckt bleibt und somit wieder einsetzbar ist. Ein Beispiel für die Tarnung ist der Conficker Wurm, der bis zu seiner ersten Entdeckung im Oktober 2008 über 370,000 Computer infizierte. Die geschätzte Nummer an Betroffenen bis zum Januar 2009 reicht von 9 Millionen bis 15 Millionen. Damit ist er der größte Wurm der zur Zeit bekannt ist, seit dem Welchia Wurm 2003. Inzwischen gibt es aber genügend Werkzeuge für seine Entfernung.[3]

Persistence hingegen, ist die Wahrscheinlichkeit dafür, dass eine unbenutzte Ressource auch weiterhin unentdeckt bleibt. Die Vulnerabilität wird also nicht behoben, und der Exploit kann weiterhin benutzt werden. Natürlich ist es auch schwer für diese beiden Variablen feste Werte zu finden, allerdings kann man anhand von vorangegangen Attacken und Beispielen ungefähre Schätzwerte festlegen. So liegt die Durchschnittliche Haltbarkeit von Zero – Day – Lücken bei 312 Tagen. Allerdings kann diese auch wesentlich länger sein. So wurden bei den Browsern Chrome und Firefox in 3 Jahren, nur eine geringe Anzahl an Lücken unabhängig entdeckt. Was die Persistence nahezu auf 1 heben würde.

Natürlich hängen diese beiden Variablen nicht nur von der Qualität des Exploits ab, sonder auch davon, wie wachsam und gut geschützt das gewählte Ziel ist. Gegen jemanden der seine Sicherheitspatches stets up – to – date hält ist die Persistence geringer, als gegen ein Ziel das seine Sicherheit vernachlässigt.Gleichwohl ist die Stealth höher gegen ein Ziel, welches wenig Wachsamkeit zeigt.

2.1.3 Der richtige Zeitpunkt

Die letzte Variable die noch zu berücksichtigen ist, stellt die Discount Rate *w* dar, in unserem Sinne die Inflation. Der Wert einer Information ist also im nächsten Jahr, nicht mehr genau so interessant, wie er es zum jetzigen Zeitpunkt ist. Die Rate liegt also immer im Bereich zwischen 0 und 1.

Das einzige was nicht unter der Kontrolle des Angreifers liegt ist der Einsatz. Deswegen ist es sinnvoll so lange mit den Nutzen der Ressource zu warten, bis dieser hoch genug ist dass man sie aufgeben kann. Also legt man eine Grenze fest, ab deren Überschreiten es sich lohnt zu zuschlagen. Dabei ist der Gewinn *G(T)*, den man bei linearem Einsatz zieht, nur bei einem Grenze von *a* oder *b* anzugreifen: *G(T) = (a + b) / 2*. Je geringer man also die Grenze setzt, desto öfter kann man seine Ressource zwar einsetzen, aber dadurch bleibt der durchschnittliche Gewinn ebenfalls klein. Das grundlegende Problem ist, die Ressource möglichst oft einzusetzen, aber sie gleichzeitig für Zeiten sparen, in denen viel auf dem Spiel steht.

Wird die Ressource zum jetzigen Zeitpunkt eingesetzt, ergibt sich ihr Wert *V* aus dem erwarteten Gewinn dieses Nutzen und dem Zukunftswert, der von der Stealth *S* sowie der Discount Rate abhängt. Damit folgt für die akute Nutzung: *V(Nutzung der Ressource) = G(T) + w S V* .Hebt man sich die Ressource auf, so errechnet sich der Wert aus der Wahrscheinlichkeit, dass sie auch weiterhin Bestand hat, und ebenfalls der Disount Rate. Folglich ist hier die Gleichung: *V (Aufsparung der Ressource) = w P V* .Die Chance dass eine Ressource eingesetzt wird, ist die Wahrscheinlichkeit *Pr* dafür, dass der aktuelle Einsatz mindestens so groß ist wie die festgelegte Grenze, *Pr(s >= T).* Analog dazu ist die Chance, dass sie aufgespart wird, die Gegenwahrscheinlichkeit, *1 - Pr(s >= T)*

Setzt man die einzelnen Bestandteile zusammen, erhalten wir unseren erwarteten Wert der Ressource:

$$V = Pr(s \geq T)(G(T) + w\,S\,V) + (1 - Pr(s \geq T))\,w\,P\,V$$

Natürlich ist es sinnvoller den Wert auf einer Seite gesondert zu haben, denn schließlich weiß der Angreifer nur Stealth, Persistence und eine selbstgewählte Verteilung des Einsatzes. Deswegen erhalten wir nach Umformen unserer ursprünglichen Gleichung.

$$V = \frac{(Pr(s \geq T)\,G(T))}{((1 - w * P) + Pr(s \geq T)\,w(P - S))}$$

Es ist nun möglich den Wert einer Ressource anhand dieser Formel zu berechnen. Aus diesem Wert lässt sich schließen, wann der beste Zeitpunkt gekommen ist anzugreifen.

2.2 Anwendung des Modells

Wir wenden nun die Rechnung zum besseren Verständnis an. Zuerst an einem einfachen Beispiel, in dem der Einsatz linear verteilt ist. Die Dringlichkeiten 1, 2, 3 ,4 ,5 ,6 des Einsatzes treten alle mit gleicher Wahrscheinlichkeit auf. Außerdem sei die Disount Rate auf 0.8 festgelegt und die Stealth auf 40% der Persistence. Wendet man nun die Formel an, sieht man wie sich die Persistence auf den optimalen Grenzwert auswirkt. Die verschiedenen Ergebnisse sind in Tabelle 1 dargestellt. Um die Rechnungen nachzuvollziehen, wird im Folgenden gezeigt wie wir auf den Wert der Tabelle im Feld 0,1 – 1 kommen. Unser *G(T)* ist in diesem Fall *(1+2+3+4+5+6) / 6 = 3,5*. Da unser Grenzwert eins ist, nutzen wir die Ressource bei jeder Gelegenheit also ist *Pr (s>= T) = 1*. Die Restlichen Werte sind bekannt, also ist es nun simples Einsetzen.

$$V = \frac{(1 * 3{,}5)}{((1 - 0{,}8 * 0{,}1) + 1 * 0{,}8(0{,}1 - (0{,}4 * 0{,}1)))} = 3.616$$

doi: 10.2313/NET-2015-03-1_03

T	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
6	1,08	1,17	1,28	1,4	1,56	1,76	2,02	2,36	2,84	3,57
5	1,96	2,1	2,27	2,46	2,7	2,98	3,32	2,76	4,32	5,09
4	2,65	2,81	3	3,22	3,47	3,77	4,11	4,53	5,04	5,68
3	3,15	3,32	3,5	3,71	3,95	4,21	4,52	4,87	**5,28**	**5,77**
2	3,47	3,62	3,79	3,97	**4,17**	**4,39**	**4,63**	**4,9**	5,2	5,56
1	**3,62**	**3,74**	**3,87**	**4,01**	4,17	4,33	4,51	4,7	4,92	5,15

Tabelle 1. Die Auswirkungen der Persistence

Die Spalten stehen für die derzeitige Persistence und die Zeilen für den Grenzwert

Aus den Ergebnissen lässt sich herauslesen, dass je höher die Persistence ist, desto länger es sich lohnt mit dem Angriff zu warten. Hat man jedoch eine geringe Persistence empfiehlt es sich die Ressource sofort zu nutzen. Logisch ist das ebenfalls verständlich, denn die Wahrscheinlichkeit dass die Ressource verfällt, auch bei Nichtnutzung, ist sehr hoch. Auch bei anders gewählten Zahlenbeispielen stieg der optimale Grenzwert, als die Persistence sich vergrößerte. Die nächste Tabelle zeigt den Effekt den die Stealth auf den optimalen Grenzwert hat. Dabei gehen wir von einer konstanten Persistence von 0,8 aus, die Discount Rate belassen wir auf 0,8.

T	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
6	2,21	2,72	2,34	2,42	2,5	2,59	2,68	2,78	2,88	3
5	3,35	3,53	3,72	3,93	4,17	4,44	4,74	5,09	5,5	5,98
4	3,91	4,17	4,46	4,81	5,21	5,68	6,25	6,94	7,81	8,93
3	**4,09**	**4,41**	**4,89**	5,23	5,77	6,43	7,26	8,33	9,78	11,8
2	4,03	4,39	4,81	**5,32**	**5,95**	**6,76**	7,81	9,26	11,4	14,7
1	3,8	4,17	4,61	5,15	5,83	6,73	**7,95**	**9,72**	**12,5**	**17,5**

Tabelle 2. Die Auswirkungen von Stealth

Die Spalten stehen für den derzeitigen Stealth und die Zeilen für den Grenzwert

Stealth zeigt genau den gegensätzlichen Effekt. Je höher der Stealth der Ressource ist, desto mehr lohnt es sich diese möglichst früh einzusetzen. Der Sinn dahinter ist, dass der Angriff aufgrund seiner hohen Tarnung nicht entdeckt wird, und somit wesentlich öfter ausgeführt werden kann. Das soll allerdings nicht bedeuten, dass es bei hohem Einsatz sinnvoller ist nicht auf den Stealth zu achten. Sowohl Stealth als auch Persistence sind wertvolle Eigenschaften, die ein Exploit besitzen kann. Aber daraus lässt sich schließen, dass eine Ressource, die nur eine sehr geringe Tarnung hat, besser für Zeiten aufgespart werden sollte, in denen viel auf dem Spiel steht, da sie mit großer Wahrscheinlichkeit nur einmalig einsetzbar ist.

Natürlich gibt es noch den wesentlich einfacheren Fall wenn man einfach mit konstantem Einsatz rechnet. Das Risiko bleibt also immer gleich hoch, dass trifft zum Beispiel auf Kriminelle zu, deren Gewinn aus dem Hacken von Kreditkarten besteht. Genauso verhält es sich mit terroristischen Organisationen. Besteht deren Ziel einzig allein darin möglichst viel Schaden zu verursachen, werden sie nicht auf besondere Ereignisse warte, sondern so oft Anschläge verüben, wie es ihnen möglich ist. Ist der Einsatz also gleichbleibend, ist die beste Taktik seine Ressource so oft und so lang wie es geht einzusetzen.

Doch meistens sind die Einsätze wohl eher ungleich verteilt und die wichtigen Ereignisse, sind zwar sehr selten, aber falls sie eintreffen, übertreffen sie die üblichen Zustände bei weitem. So könnten die Einsätze zum Beispiel, bei 1, 4, 9, 16, 25, 36 liegen ,in Form einer Parabelfunktion, oder aber auch als exponentielle Verteilung, 1, 2, 4, 8, 16, 32. In unserem Model hätte das Einfluss auf *G(T)* und *Pr(s >= T)*. Gehen wir einmal von einer exponentiellen Verteilung aus, so wäre *G(32) = 32*, aber die Wahrscheinlichkeit *Pr(s>=T)*, dass diese Grenze je überschritten wird, läge nur bei 1/32. Anhand des Modells, lässt sich sagen, dass je mehr die Einsätze verzerrt sind, desto mehr steigt der optimale Grenzwert. Aber desto länger muss man auch warten, bis dieser Wert überschritten wird. Gerade bei stark verteilten Einsätzen muss man allerdings darauf achten, nicht zu lange zu warten, denn dass der höchste Fall erreicht wird, ist sehr unwahrscheinlich.

T	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
32	1,1	1,22	1,36	1,55	1,8	2,13	2,63	3,43	4,93	8,77
16	13,7	14,7	15,9	17,3	19	21,1	**23,7**	**27,7**	**31,5**	**37,6**
8	**15,5**	**16,4**	**17,5**	**18,7**	**20,1**	**21,8**	23,7	26	28,9	32,4
4	14,3	15,1	16	16,9	18	19,3	20,7	22,4	24,4	26,8
2	12,6	13,2	14	14,8	15,6	16,7	17,8	19,1	20,6	22,4
1	11	11,5	12,1	12,8	13,6	14,4	15,3	16,4	17,7	19,1

Tabelle 3. Verteilte Einsätze

Die Spalten stehen für die Persistence und die Zeilen für den Grenzwert, w = 0,9 S = P/2

Bevor nun die echten Fallbeispiele kommen, lässt sich zusammenfassen, dass es 3 Faktoren gibt, die eine Ressource auszeichnen, mit deren Einsatz es sich lohnt zu warten. Diese wären, eine niedrige Stealth, eine hohe Beständigkeit und die Chance einen großen Nutzen in Fällen, in denen viel auf dem Spiel steht zu ziehen. Umgekehrt ist eine Ressource mit hoher Tarnung, aber wenig Beständigkeit besser dafür geeignet, in alltäglichen Dingen eingesetzt zu werden.

3. Geschichtliche Fallbeispiele

3.1 Iranischer Angriff auf Saudi - Aramco

Bei diesem Angriff war die Saudi – Arabischen Ölfirma Saudi Aramco das Ziel. Diese ist die derzeit größte Erdölfördergesellschaft der Welt und fördert jährlich 525,0 Mio. Tonnen Erdöl. Die Financial Times nannte die Firma mit 10 Billion US – Dollar Unternehmenswert sogar das wertvollste Unternehmen der Welt.[4] Am 15ten August 2012 infizierte ein Computervirus die Firma, und befiel ungefähr 30.000 windowsbasierte Rechner. Später wurde dieser Shamoon getauft.

Seine Hauptfunktion bestand wohl darin Daten von Computerfestplatten zu löschen. Der Virus bestand dabei aus 3 Teilen, einem Dropper, der sich auf den Hauptteil bezog und Quelle der Infektion war, einem Wiper – Modul, das für die Zerstörung der Daten zuständig war und einem Reporter Modul, das die Infektion an den Angreifer zurückmeldete. Der Virus überschrieb dabei die Daten mit einem Bruchteil eines Bildes, das eine brennende amerikanische Flagge zeigte.[5] Obwohl der Virus erfolgreich 75% der Arbeitsstationen infizierte[6] beschädigte er nicht die kritische Infrastruktur, da diese auf isolierten System lagen. Es gab also keinen Ölverlust oder Explosionen, dennoch ist davon auszugehen dass Bohr und Produktionsdaten verloren gegangen sind.

Obwohl es einer der größten Angriffe auf eine einzelne Firma war, blieb also der große Schaden aus. Das lag vor allem daran dass die Attacke nicht sehr unauffällig vorging und schnell gestoppt wurde. Nach 4 Tagen war der Virus komplett entfernt. Zuerst bekannte sich eine Hackergruppe mit dem Namen „Cutting Sword of Justice“ zu dem Angriff, allerdings wurde nach genaueren Recherchen klar dass die Quelle aus dem Iran kam. Die Regierung lehnte zwar jegliche Verantwortung ab, aber die Kontrolle über das Internet im Iran ist so streng, dass es schwer vorstellbar ist, dass sie davon nichts gewusst hätte. Ebenfalls dafür spricht, dass der Iran kurz davor selber von einer Attacke getroffen wurde, dem Stuxnet, welche dem iranischen Atomprogramm schadete. Vermutlich fühlte sich der Iran dazu gedrängt schnell eine ebenbürtige Antwort zu senden , um nicht als schwach angesehen zu werden. Das erklärt auch einige Fehler im Virus. Die niedrige Stealthrate und die Tatsache, dass viel auf dem Spiel stand, decken sich ebenfalls mit unserem Modell, was unter solchen Bedingungen auch den sofortigen Einsatz einer Ressource vorschlägt.

Jedoch war der Angriff auch gleichzeitig ein Weckruf an die Firma ihre Sicherheit zu erhöhen. Saudi Aramco deckt ein Zehntel des Weltbedarfs an Öl.[7] Sollte deren Produktion stark geschädigt werden, wäre das ein internationaler Schaden. Das zeigt noch einmal was für eine Bedrohung Cyber Conflict darstellt.

3.2 Tägliche E-Spionage Chinas

China stellt eine außergewöhnlich Rolle im Cyberkrieg dar. Zwar besitzt keine Nation eine reine Weste und jegliche Verknüpfung mit E-Spionage wird verleugnet, was dazu geführt hat, dass diese Aussage nur noch als Fiktion angesehen wird, dennoch übertrifft China viele seiner Konkurrenten. Einigen Schätzungen zufolge haben 90% der Angriffe die in der USA erfolgen ihren Ursprung in China(8). Dabei scheint dass Hauptziel der Diebstahl von Technologie zu sein, aber gleichzeitig besteht auch die Gefahr dass die militärischen Kapazitäten eines Landes ans Licht geraten. Ein 2013 veröffentlichter Report des Pentagons besagt, dass die China inzwischen soviel in seine Cybertechnologien investiert hat, dass es nun eine führende Rolle einnimmt. Dabei belaufen sich die Ausgaben von China selbst für Abwehrstrategien auf 135 bis 215 Milliarden Dollar, dies ist aber sogar mit den höchsten Werten nur ein Drittel dessen was die USA investiert.[8] Aber auch China beschuldigt die USA Spionage zu betreiben, eine Anschuldigung, die auch durch die Leaks von Edward Snowden bekräftigt wurde. Am 5. Mai 2014 klagte die USA chinesische Offiziere wegen Wirtschaftsspionage an. Als Gegenantwort rief China den US- Außenbotschafter zu sich. Dies sind natürlich alles vorerst symbolische Akte, es wird weiterhin auf Verhandlungen gesetzt. Aber das Verhältnis zu China bleibt dadurch angespannt. Tom Denilon, der Sicherheitsberater nannte das Lösen dieser Probleme den Schlüssel für ein zukünftiges gutes Verhältnis zu China.[9] US – Justizminister Holder meinte, außerdem dass der wirtschaftliche Erfolg eines Landes nicht davon abhängen dürfe, wie gut deren Ressourcen zur Spionage genutzt werde.[10]

Ein Grund dafür, dass China so oft erwischt wird, bei ihren Versuchen an Informationen zu gelangen, liegt daran dass die Stealth oft nur sehr durchschnittlich gehalten wird. Das wird zum Einen, durch die Vielzahl an Attacken ausgeglichen, sodass manche Ziele überlastet sind, zum Anderen, ist nicht jedes Ziel auf dem neuesten Stand der Technik.

Betrachten wir die chinesischen Angriffen anhand unseres Modells, scheint der häufige Einsatz der Ressource nicht gerechtfertigt, da der Einsatz im Moment doch sehr gering ist. Inzwischen ist China kein Entwicklungsland mehr und stellt auch eine starke wirtschaftliche Macht dar, womit der technologische Informationsgewinn nicht mehr so hoch ist, wie er es vor 20 Jahren war. Ebenfalls gibt es keinen militärischen Konflikt mit anderen Ländern. Ein möglicher Grund warum sie nicht warten, ist, dass sie bei all ihren Ressourcen von geringer Überlebensdauer ausgehen, also niedriger Persistence. Eventuell besitzt China auch ausreichend bessere Ressourcen, sodass es ihnen nicht schadet, die schwächeren sofort und oft einzusetzen. Eine letzte Überlegung ist noch, dass sie sich gegen schlechter geschütztere Zielen eine höhere Stealth erwarten, und somit über mehrere Jahre Informationen sammeln können. Die hohe Stealth einer Ressource schlägt wie Tabelle 2 zeigt einen häufigen Einsatz dieser vor.

3.3 Frühzeitiger Einsatz einer Ressource am Beispiel China

In den vorangegangenen Beispielen, fand der Einsatz einer Ressource immer zum erwarteten Zeitpunkt statt, gemessen an unserem Modell. Doch es gibt auch Ereignisse in denen Länder zu früh gehandelt haben, dabei muss es sich bei der Ressource nicht immer um einen Cyberexploit handeln. So geschehen, bei dem Exportstopp Chinas von seltenen Erdelementen um wirtschaftlichen Druck auf Japan auszuüben.

Zu den Seltenen Erdelementen zählen insgesamt 17 Elemente. Deren Name rührt daher, dass große Lagerstätten, also Ansammlungen von diesen selten sind. Ein Großteil der Gewinnung, besteht daher aus der chemischen Aufbereitung bei Metallen, die häufiger in der Erden vorkommen. Folglich ist es sehr aufwändig Minen zu errichten und die seltenen Erdelemente zu gewinnen. Bis in die 1980er Jahre hinein, war die US führender Produzent, stellte dann allerdings immer mehr den Minenbetrieb ein, denn zu diesem Zeitpunkt wurden sie hauptsächlich für Forschung oder ganz spezielle Aufträge verwendet. Andere Länder folgten diesem Beispiel. Nur China widerstand der Versuchung und hielt die Produktion aufrecht, was damals wenig Sinn zu ergeben schien.[11] Heutzutage werden seltene Erdmetalle in vielen Schlüsseltechnologien eingesetzt. Sie finden ihre Anwendung in Solaranlagen, Computerbildschirmen, Legierungen und vielen weiteren Bereichen. Lange Zeit war der chinesische Export billiger als selbst wieder in Eigenproduktion zu treten. Im Jahr 2009 wurden 124.000 Tonnen von ihnen verwendet, mit jährlich steigender Nachfrage. China hat auf das richtige Pferd gesetzt und nimmt einen Anteil von über 90% an

den Exporten von seltenen Erdmetallen ein. Diese Monopolstellung erweist sich in unserem Fall als wichtiges Druckmittel.

Am 7. September 2010 kollidierte ein Fischerboot mit 2 Japanischen Küstenwache Schiffen im Seegebiet nahe den Senkaku Inseln.[12] China und Japan streiten schon länger um diese Inseln, deswegen nahmen die Japaner die chinesische Besatzung in Gewahrsam. Nachdem China am 9. und 12. September die Freilassung der Gefangenen gefordert hatte, entließ Japan die Crew, der Kapitän wurde weiterhin zurück gehalten. Die Spannung kochte weiter hoch, bis China am 21. September ohne Vorwarnung alle Exporte von seltenen Erdelementen einstellte. Wegen ihres großen Exportanteils, waren die Auswirkungen weltweit spürbar. Japan beschwerte sich zwar über diese ökonomische Kriegsführung ließ den Kapitän aber dennoch frei, nach 3 weiteren Tagen. Es dauerte 1 Monat bis China den Export wieder aufnahm, und 2 Monate bis wieder nach Japan geliefert wurde.

Dieser Zwischenfall war ein Weckruf für andere Länder und so wurde wieder in die Förderung von seltenen Erdelementen investiert. In den USA ist die Mountain Pass Mine bald wieder bereit für die Produktion, in Japan arbeitet man an der Förderung von Unterwasservorkommen und auch Australien hat viele Minen wieder geöffnet. Hat China also falsch gehandelt?

Unser Modell legt diese Vermutung nahe, schließlich hatte China seine Monopolstellung schon lange Zeit, ohne dass jemand etwas dagegen unternommen hat. Die Persistence lag also sehr hoch, und die Ressource hätte sehr wahrscheinlich noch länger Bestand gehabt. Des weiteren war die Stealth sehr gering, der Engpass an seltenen Erdelementen fiel sofort aus. Zwar bestritt China jeglichen politischen Zusammenhang, die Verbindung war aber zu offensichtlich. Das wiederholte Stoppen des Exports, ist nun auch erschwert, da andere Länder nun versuchen unabhängig zu werden. Die Frage ist, ob das zurückgewinnen der Gefangenen den Einsatz einer so wertvollen Ressource wirklich wert war, wenn zukünftige Situationen wesentlich größere Gewinne bieten.

4. Ausblick in die Zukunft

4.1 Zero – Day – Exploits als Geschäft

Zu Beginn des Cyberkrieges erfuhren Firmen ihre Schwachstellen kostenlos, meistens aus dritter Hand. Sei es aus Foren oder Usermeldungen. Doch mit der steigenden Bedeutung von Exploits, begann sich ein Markt zu entwickeln, mit Preisen für einen Zero – Day – Exploit die über 100.000 US Dollar liegen.

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Bild 2: Jeder Preis setzt die neueste Version an Software und einen Exklusivverkauf voraus, plus die Bedingung den Hersteller nicht mehr zu alarmieren[14]

Heutzutage stellt das einen cleveren Hacker vor schwere Entscheidungen. Er kann falls er eine Schwachstelle entdeckt, diese dem Hersteller melden, und somit sein Ansehen steigen und als Berater einsteigen. Er kann zu einer Sicherheitsfirma gehen, die ihm Geld für diese Information bietet, und damit auch die Schwachstelle beheben. Oder er wendet sich an einen Makler, der einen Deal mit der Regierung eines Landes arrangiert und somit vermutlich den größten Profit herausschlägt.(14) Deswegen verkaufen viele talentierte Hacker, die einst Microsoft oder andere Firmen warnten, die entdeckten Schwachstellen an den Höchstbietenden. Dabei gehen die Schwachstellen häufig an den Westen, denn in China sind genügend einheimische Hacker, welche die Preise drücken und in Russland ist die Kriminalität zu hoch. Fakt ist, die besten Preise erhält man in Amerika und Europa. Zwar bieten auch die Softwarehersteller selber Belohnungen an, können aber in diesen Preissegmenten nicht mithalten. So bietet Google maximal um die 3200 US – Dollar für die komplexesten Fehler in ihrer Software.[14]

In diesem Schwarzmarkt ist die USA der größte Käufer. Jedoch nutzen die USA diese Informationen nicht zur Verteidigung, sondern verfolgen die Strategie, durch diese Exploits selber ihr Potenzial im Cyberkrieg zu steigern. Laut dem ehemaligen Berater des Weißen Hauses für Cybersecurity Richard Clarke, lege die USA zu viel Wert auf ihre offensiven Möglichkeiten, was Konsumenten und Firmen in Gefahr brächte.[13] Hat also eine fremde Macht Zugriff auf die selbe Ressource, ist ein Unternehmen wie Microsoft schutzlos ausgeliefert, obwohl die Regierung theoretisch die Möglichkeit hätte Vorsorge zu treffen. Außerdem besteht die Gefahr dass nach eigenem Einsatz einer Ressource, diese schnell dupliziert und vice-versa eingesetzt werden kann, was wieder einheimische Unternehmen in Bedrängnis bringt

Dabei ist der Markt noch lange nicht gesättigt. Selbst in Software, die häufig genutzt wird und weit verbreitet ist, werden immer wieder neue Schwachstellen gefunden. Wieder dienen hier Browser als Beispiel, so wurden in Firefox 400 und in Chrome sogar 800 Lücken gefunden von 2009 – 2012. Mit der Weiterentwicklung von Software, zum Beispiel durch Patches um Schwachstellen zu beheben oder neue Features einzuführen, entstehen ständig neue Möglichkeiten Zero – Day – Exploits zu entdecken.

Mit dem steigenden Interessen von Staaten an solchen Exploits, steigen auch die Anzahl an unabhängigen Entdeckungen. Das hat laut unserem Modell mehrere Folgen. Zum einen sinkt die Persistence, da es immer wahrscheinlicher ist, dass ein neuer Hacker die Schwachstelle entdeckt und sie somit bekannt wird. Das führt dazu dass Ressourcen wesentlich eher genutzt werden, weil die lohnenswerte Grenzen sinkt. Zum anderen sinken durch steigendes Angebot selbstverständlich auch die Preise. Howard Schmidt, der wie die gleiche Position wie Richard Clarke inne hatte, nannte es naiv zu glauben dass man längere Zeit als einziger Zugriff auf einen Zero – Day – Exploit hat.

4.2 Cyberkrieg als ernste Gefahr

Die Bedeutung, die Cyberkrieg, einnimmt ist nicht zu unterschätzen. Besonders in unseren modernen Zeiten, in denen die meiste Infrastruktur aus Software besteht. Der Fall Saudi – Aramco hat gezeigt, welche globalen Auswirkungen möglich sind, sollte ein Angriff Erfolg haben. Ebenfalls besteht die Gefahr dass Terrorgruppen an besonders wertvolle Exploits gelangen, und

doi: 10.2313/NET-2015-03-1_03

diese nicht zu lange aufheben, sondern einfach darauf aus sind Schaden zu verursachen. Es existieren zwar schon Übereinkünfte zwischen den Staatengemeinschaften, diese werden aber von niemandem Ernst genommen. Notwendig ist ein allgemeines Umdenken, welche Gefahr solche Exploits bieten. Wird zum Beispiel ein Atomkraftwerk lahmgelegt, könnte dies schnell zu verheerenden Auswirkungen in einem Land führen. Die NATO hat bereits das Cooperative Cyber Defence Centre of Excellence gegründet um besser geschützt zu sein gegen solche Maßnahmen. Dieses dient zur Beratung in kritischen Fragen, versucht Forschungsarbeiten zu publizieren und arbeitet an einem rechtlichen Rahmen zur Cyberverteidigung. Eine Möglichkeit die Gefahr zu verringern wäre, sich auf eine Abrüstung für Cyberwaffen zu einigen wie es bereits mit anderem Kriegsgerät geschehen ist.

4.3 Anwendung des Modells in Spielen

Ein Modell, das von so vielen Überlegungen und Variablen abhängt ist prädestiniert für Strategiespiele. Spionage ist bereits ein oft genutztes Mittel in Spielen. Der interessante Faktor den uns das Modell bietet ist, dass man alle Ressourcen im vornherein festlegen kann und so ziemlich genau den Wert einer jeden errechnen kann. Spieler können nun extra Belohnungen erhalten je näher sie dem Idealwert kommen beim Einsatz. Das ganze ist natürlich einfacher in einem PvE Universum, da so nicht besonders auf das verhalten des Computers Rücksicht genommen werden muss. Am ehesten wäre der Einsatz in Spielen wie Civilization (Strategie - Simulationsspiel) denkbar, da dort durch das Durchschreiten verschiedener Zeitepochen viele Ressourcen denkbar sind und sich so nicht allzu schnell ein gewissen Schema einspielt.

Wesentlich komplexer wäre der Einsatz in groß angelegten Online Spielen a la EVE Online, die ebenfalls sehr simulationslastig sind. EVE Online ist ein MMORPG, welches im Weltraum stattfindet und sich auf Handel und Kampf der unterschiedlichen Fraktionen untereinander konzentriert. Das hier bereits annähernd echte politische Gebilde vorherrschen, zeigt sich in den vielen Allianz Kriegen oder auch groß angelegten Diebstählen, die es teilweise sogar in die Medien schaffen.[15] Des weiteren herrscht dort bereits ein funktionierendes Wirtschaftssystem. Ein realistisches Modell zur Einschätzung von Profit beim Hacking oder Sabotieren würde dem Spiel gewiss einen neuen Schuss Realismus verschaffen.

Eine letzte Möglichkeit wäre die Anwendung in Serious Games, um Situationen der Wirklichkeit nachzustellen. Allgemein lassen sich viele neue Ansätze finden, die dem Realismus in Spielen Auftrieb verschaffen können.

5. Zusammenfassung

Diese Arbeit sollte ein grundlegendes Verständnis über Cyberkonflikt vermittelt haben. Dieser hat schon seit längerem begonnen und sollte nicht unterschätzt werden. Das Eindringen in Schwachstellen kann sowohl zum positiven genutzt werden, wie zur Verbrechensbekämpfung oder Vorbeugung von Angriffen, gleichzeitig kann aber auch der Spieß umgedreht werden und Nationen geraten in starke Gefahr. Die Bedeutung wird in Zukunft sehr wahrscheinlich eine noch größere Rolle spielen. Die Ergebnisse aus unserem Modell zeigen, dass sowohl Persistence als auch Stealth wichtige Attribute für einen Exploit sind. Die gegensätzliche Effekte dieser zwei auf den optimalen Zeitpunkt sind auch deutlich hervorgegangen, wie in 2.2 behandelt. Genau so spielt auch die Verteilung der Einsätze eine große Rolle. Wichtig ist nicht den Fehler zu machen, seine Schwachstellen in Bezug auf das zu sehen was selber auf dem Spiel steht. Einem Angreifer reicht der derzeitige Zustand an Einsätzen vielleicht bereits aus um zuzuschlagen. Ebenso so wichtig ist es dass der Gewinn sich nicht nur aus dem direkten Nutzen ableitet, sonder auch unerwünschte Nebeneffekte auftreten können. Bei Entdeckung steigt automatisch die Wachsamkeit des Zieles und politische Konsequenzen können folgen. Herrscht Kriegszustand zwischen zwei Parteien gilt es die Risiken noch genauer abzuwägen. Dennoch ist es weiterhin schwer abzuschätzen welchen Wert die Persistence und Stealth einer Ressource besitzen. Hier kann man nur Maßstab an bereits existierenden Quellen und Beispielen nehmen. Weiterhin ist immer noch schwer zu sagen wie schnell eine Schwachstelle behoben wird. Auch hier dienen nur Studien als Maßstab.

6. Quellenangabe

[1]http://www.cyberconflict.org/blog/2013/8/1/what-are-the-costs-of-cyber-crimes-and-cyber-espionage.html

[2]http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

[3]http://en.wikipedia.org/wiki/Conficker

[4]http://de.wikipedia.org/wiki/Saudi_Aramco

[5]http://bakerinstitute.org/files/641/

[6]http://www.darkreading.com/attacks-and-breaches/saudi-aramco-restores-network-after-shamoon-malware-attack/d/d-id/1105991?

[7]http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0

[8]http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html?pagewanted=all&_r=0

[9]Donilon T (2013) Press Briefing By National Security Advisor Tom Donilon (The White House, Washington)

[10]http://www.n-tv.de/politik/China-bestellt-US-Botschafter-ein-article12862406.html

[11]http://www.dailytech.com/World+Trade+Org+to+China+on+Rare+Earth+Metals+Stop+Breaking+the+Law/article34597.htm

[12]http://en.wikipedia.org/wiki/2010_Senkaku_boat_collision_incident

[13]http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510

[14]http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

[15]http://www.t-online.de/spiele/id_19390698/milliardenraub-in-onlinespiel-eve-online-.html

[16]http://searchsecurity.techtarget.com/feature/Private-market-growing-for-zero-day-exploits-and-vulnerabilities

[17]http://m.eet.com/media/1154886/25731-electronics_industry_braces_for_rare_earth_materials_shortages_pdf.pdf

[18]http://www.pnas.org/content/111/4/1298.full.pdf+html

doi: 10.2313/NET-2015-03-1_03