St. Pölten University of Applied Sciences

/informatik & security

/fh/// st.pölten

Cyber-Terrorismus

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur

eingereicht von

SZING Marcus BSc
is181833

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer: FH-Prof. Mag. Dr. Simon Tjoa

Ort, TT.MM.JJJJ

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Ort, TT.MM.JJJJ

(Unterschrift Autor/Autorin)

Danksagung

Ich möchte mich an dieser Stelle bei allen Personen bedanken, die mich bei der Erstellung dieser Arbeit mit allen Kräften unterstützt haben.

Ich möchte mich besonders bei meinem Betreuer Herrn Mag. Dr. Simon Tjoa dafür bedanken, dass Sie sich im letzten Jahr immer wieder die Zeit genommen haben den Fortschritt meiner Arbeit regelmäßig zu begutachten und mit mir die Fortschritte zu besprechen, sowie Verbesserungsvorschläge zu äußern. Die Arbeit hätte ohne Sie nicht die Qualität und Tiefe erreicht, die sie nun bietet.

Besonderer Dank gilt auch dem Team der Bibliothek der Fachhochschule St. Pölten für die Unterstützung bei der Beschaffung verschiedener wissenschaftlicher Arbeiten, sowie für die Übernahme der angefallenen Kosten. Ich möchte hier speziell Herrn Rathmanner Karl für seine Hilfsbereitschaft und sein Engagement danken.

Zusätzlich bedanke ich mich bei meinen Studienkollegen Herrn Dominik Burak BSc und Herrn Thomas Pointner BSc für die Unterstützung und die gute Zusammenarbeit.

Schließlich möchte ich mich bei meiner Familie, die die gesamte Zeit hinter mir gestanden ist und mich so gut wie möglich unterstützt hat, bedanken.

Zusammenfassung

Eine funktionierende IT ist für viele Bereiche der Gesellschaft von großer Bedeutung. Diese digitale Vernetzung, bietet nicht nur Vorteile, sondern sie bietet Hackerinnen und Hackern die Möglichkeit Cyber-Angriffe zu auf die IT-Infrastruktur zu starten. In dieser Arbeit soll auf eine bestimmte Form von Cyber-Angriffen eingegangen werden, nämlich Angriffe von Cyber-Terroristinnen und Cyber-Terroristen. Mit der zunehmenden Digitalisierung und der Präsenz des Internets haben sich auch neue Möglichkeiten und Wege für Terroristinnen und Terroristen ergeben Anschläge zu verursachen, Ideologien zu verbreiten und ihre Vorstellungen umzusetzen. Im Zuge dessen werden einige bereits aufgetretene Fälle von Cyber-Terrorismus näher betrachtet und die wichtigsten Informationen aufbereitet. Konkret werden neun ausgewählte Fälle der vergangenen 22 Jahre behandelt. Durch den entstehenden Überblick werden zunächst Parallelen zwischen den Fällen sichtbar gemacht. Anschließend werden aus den gewonnen Erkenntnissen Techniken entwickelt, die von Regierungen und Unternehmen genutzt werden können, um sich vor terroristischen Angriffen über das Internet zu schützen. Diese Techniken orientieren sich an bereits existierenden kriminologischen Ansätzen der analogen und virtuellen Welt. Außerdem wird erläutert, welche Aspekte es bei cyber-terroristischen Angriffen zu beachten gilt und wie das bereits existierendes Framework STIX (Structured Threat Information Expression) für Cyberkriminalität sich mit Cyber-Terrorismus vereinbaren lassen.

Abstract

A functioning IT-service is essential for many areas of modern society. This digital interconnectivity not only provides advantages, but also a possibility for hackers to start cyber-attacks on the IT-infrastructure. This work concentrates on certain type of cyber-attacks, specifically cyber-terrorism. Due to the increasing digitalization and the presence of the internet terrorists gained new possibilities to launch their attacks, spread their ideologies and realize their ideas. In the course of this some existing cases of cyber-terrorism were taken to a closer look and essential information was prepared. Specifically, nine cases from the past 22 years are addressed. Through the resulting overview, parallels between the cases became visible. In the next step this knowledge was taken to develop techniques companies as well as the government may use to protect themselves from attacks through the internet launched by cyber-terrorists. These techniques are based on already existing criminological approaches of the analog and virtual world. In addition to this it is explained which aspects are important to take note of when dealing with a case of cyber-terrorism. The already existing STIX (Structured Threat Information Expression) framework for cybercrime was further examined about how effective it is in order to describe cases of cyber-terrorism.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung Cyber-Terrorismus

Weltweit nutzten 2018 rund 3,9 Milliarden Personen das Internet, was einen Anteil von 55,6% der Weltbevölkerung ausmacht [1]. Für das Jahr 2021 wurde bereits ein Anstieg auf etwa 4,14 Milliarden Nutzerinnen und Nutzern prognostiziert [1]. Nicht alle Inhalte des Internets sind dabei immer harmlos, sondern können von terroristischen Organisationen stammen, die zum Beispiel für ihre Zwecke werben. Allein Twitter sperrte im Zeitraum August 2015 bis September 2017 936 000 Profile mit Terrorbezug [2] und auch Facebook entfernte im 1. Quartal 2019 6,4 Millionen Inhalte mit Terrorverdacht [3].

In den sozialen Medien sind Terroristinnen und Terroristen bereits angekommen. Doch das Internet kann von ihnen auch genutzt werden, um Cyber-Angriffe gegen Unternehmen und Staaten zu starten. Laut einer Statistik sind europaweit sehr viele Unternehmen an das Internet angebunden [4] und besitzen damit erreichbare Infrastruktur für Terroristinnen und Terroristen. In acht Ländern, darunter auch Österreich, beträgt laut [4] der Anteil an Firmen mit Internetzugang 100%. Dazu kommt, dass die Tendenz zu angezeigten Fällen bezüglich Cybercrime steigt [5]. Immerhin 39,4% der österreichischen Bevölkerung sorgen sich um die Risiken eines Terroranschlags [6].

Sowohl seitens der Europäische Union [7], als auch vom Außenministerium der Vereinigten Staaten von Amerika (USA) [8] gibt es Listen mit Organisationen, die für ihre terroristischen Handlungen bekannt sind. Diese Listen umfassen alle aktuellen Terror-Organisationen und nicht nur jene, die ausschließlich oder unter anderem für Cyber-Terrorismus bekannt sind.

Terroristische Organisationen sind ein Problem, da sie im Zuge ihrer Anschläge immer wieder die Tode vieler Personen zu verantworten haben [9]. Viele Unternehmen sind mit dem Internet vernetzt [4], und somit von außen erreichbar. Daher ist nicht auszuschließen, dass sie Opfer eines Hacking-Angriffs werden und somit ins Ziel terroristischer Vereinigungen geraten. Im Zuge dieser Arbeit soll ein Überblick über cyber-terroristische Angriffe der letzten Jahre entstehen. Durch Aufbereitung und Analyse der Fälle, soll der Frage nachgegangen werden, welche Fälle von Cyber-Terrorismus es in den letzten Jahren gab und welche Gemeinsamkeiten, Auffälligkeiten, Unterschiede, Ursachen, Folgen und sonstige Fakten dazu gab beziehungsweise gibt es? Durch Beantwortung dieser Fragen sollen Faktoren herausgearbeitet werden, die die bisherigen Ziele charakterisierten und somit Eigenschaften darstellen, die dazu beitragen, dass die Wahrscheinlichkeit für einen cyber-terroristischen Angriff erhöht ist. Außerdem soll der Frage nachgegangen werden, ob es bereits existierende Frameworks gibt, die zur Beschreibung von Cyber-Terror-Fällen genutzt werden können? Dies soll dabei helfen potenzielle zukünftige Opfer zu erkennen, damit diese Maßnahmen ergreifen können, um einerseits ihre Attraktivität als Ziel zu verringern und andererseits Sicherheitsmaßnahmen zu implementieren, die einen erfolgreichen Angriff erschweren. Ziel ist es eine Übersicht von Techniken auszuarbeiten, die die wesentlichen Maßnahmen beinhaltet.

1.1. Begriffserklärungen

Da der Begriff nicht eindeutig definiert ist, wird in diesem Abschnitt der Begriff Cyber-Terrorismus für die Arbeit näher definiert und von den verwandten Begriffen Cyber-Warfare und Hacktivismus abgegrenzt.

Zunächst findet sich im Cyber-Terrorismus, das Wort Cyber wieder. Das Wort „Cyber“ bezeichnet laut [10] „die von Computern erzeugte virtuelle Scheinwelt […]“. Laut [11] lässt sich der Begriff auf den US amerikanischen Autor William Gibson zurückführen, welcher in seinen Romanen unter anderem den Begriff Cyberspace erwähnt und ihn als eine virtuelle Realität beschreibt, welche den Menschen eine Art zweite soziale Handlungsumgebung neben der realen Welt bietet. Konkret wäre hier das Buch „Burning Chrome“ [12] aus den 1980er Jahren zu erwähnen, welches damals bereits eine Welt beschrieb, die mittlerweile Realität ist, wenn man soziale Netzwerke betrachtet. Aus diesen Definitionen heraus, soll für diese Arbeit der Begriff „Cyber“ Großteils für das Internet und alle Komponenten und Dienste stehen, welche diese virtuelle Realität bilden.

Wenn man von Cyber-Terrorismus spricht, spricht man von Terror. Es ist daher wichtig im nächsten Schritt festzustellen, was mit dem Begriff „Terror“ gemeint ist. Eine Bedeutung des Wortes „Terror“ findet sich in [13]. Darin wird „Terror“ als „[…] Verbreitung von Angst und Schrecken durch Gewaltaktionen […] [13]“ beschrieben.

Da Terrorismus eine Straftat ist [14] gibt es ein entsprechendes Gesetz, das Terrorismus als Straftat regelt. Für diese Arbeit wurde das österreichische Gesetz herangezogen. Die Details zum österreichischen Gesetz finden sich auf der Webseite des Rechtsinformationssystem des Bundes. Unter §278c Absatz 1 Strafgesetzbuch [14] finden sich die laut österreichischem Gesetz geltenden terroristischen Straftaten:

- Mord
- Körperverletzungen
- erpresserische Entführung
- schwere Nötigung
- gefährliche Drohung
- schwere Sachbeschädigung, Datenbeschädigung und Störung der Funktionsfähigkeit eines Computersystems, wenn dadurch eine Gefahr für das Leben eines anderen oder für fremdes Eigentum in großem Ausmaß entstehen kann oder viele Computersysteme oder wesentliche Bestandteile der kritischen Infrastruktur beeinträchtigt werden
- vorsätzliche Gemeingefährdungsdelikte oder vorsätzliche Beeinträchtigung der Umwelt
- Luftpiraterie
- vorsätzliche Gefährdung der Sicherheit der Luftfahrt
- Aufforderung zu terroristischen Straftaten und Gutheißung terroristischer Straftaten
- eine nach dem österreichischen Waffengesetz oder Kriegsmaterialgesetz strafbare Handlung

Die aufgelisteten Taten werden laut [14] als „Terroristische Straftaten“ geltend gemacht, „wenn die Tat geeignet ist, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens oder eine schwere Schädigung des Wirtschaftslebens herbeizuführen, und mit dem Vorsatz begangen wird, die Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation zu einer Handlung, Duldung oder Unterlassung zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation ernsthaft zu erschüttern oder zu zerstören.“ [14]

Bei dieser Begriffsbestimmung ist jedoch zu beachten, dass das österreichische Gesetz diese Definition mitunter deshalb erstellt hat, da dies Auswirkungen auf die Strafvollziehung hat und somit einem Straftäter ein unterschiedliches Strafmaß je nach Delikt zustehen kann. Es wird nicht näher auf die Arbeitsweise oder Funktionsweise einer terroristischen Organisation eingegangen, sondern lediglich auf die verübten Straftaten und die Ziele beziehungsweise Absichten.

Eine weitere Definition von Terrorismus findet sich in [11]. Der Autor stützt sich in seiner Arbeit auf eine Definition des Terrorismus aus [15]. Darin heißt es „Im Allgemeinen lässt sich unter Terrorismus die systematisch vorbereitete Planung und Durchführung illegaler Gewaltakte durch temporär oder dauerhaft zusammengesetzte Gruppen, die in der Regel konspirativ und subversiv, national oder international mit der Zielsetzung kooperieren, eigene oder im Auftrag zu erfüllende politische Ziele zu erreichen.“ [15] Weiters ist das Ziel dieses Terrors „[…] die Abschaffung bestehender Herrschaftsverhältnisse, die Beseitigung bestehender Herrschaftseliten und die Etablierung radikaler Alternativen unter Zuhilfenahme von Gewalt, Schrecken und Terror.“ [15]

Aus diesen Definitionen geht hervor, dass es sich bei Terrorismus meist um Gruppen handelt, die gewaltsam und/oder illegal versuchen Ihre Interessen durchzusetzen. Sie richten sich gegen die Regierung oder gegen die Bevölkerung und versuchen durch ihre Handlungen eine einschüchternde Wirkung zu haben.

1.2. Cyber-Terrorismus

Indem nun die beiden Begriffe zusammengeführt werden kommt man zum Cyber Terrorismus. Dabei handelt es sich um gewaltsame Interessensdurchsetzung über das Internet. Eine Cyber-Terroristin oder ein Cyber-Terrorist, also eine Person, die Cyber Terrorismus betreibt, versucht ihre oder seine Interessen gewaltsam durchzusetzen, indem sie oder er das Internet benutzt. Dazu benötigt sie oder er ein internetfähiges Gerät, wie einen Computer, und ein Ziel, welches ebenfalls direkt oder indirekt mit dem Internet verbunden ist. Da nun eine Verbindung zwischen dem Computer der Terroristin oder dem Terroristen und ihrem beziehungsweise seinem Ziel liegt, kann sie oder er versuchen das Ziel anzugreifen, damit ein Schaden entsteht und Ziele, wie zum Beispiel in [14] beschrieben, erreicht werden.

[16] definiert den Begriff Cyber-Terrorismus in seinem Buch genauer, indem er bereits bestehende Definitionen aufgreift, miteinander vergleicht und anschließend daraus seine eigene Definition ableitet. Eine davon stammt aus [17] und beschreibt, dass Cyber-Terrorismus politisch motiviert ist und dass das Ziel Computer, Netzwerke, Programme und Daten sind. Laut [16] fehlt dieser Definition jedoch der terroristische Aspekt der Angst, die verbreitet werden soll. Eine weitere Definition stammt aus [18], worin die Autorin Cyber-Terrorismus als gesetzeswidrige Angriffe gegen Computer, Netzwerke und die darauf befindlichen Informationen sieht. Das Ziel dafür muss laut [18] politisch oder sozial motiviert sein und die betroffene Regierung oder Bevölkerung einschüchtern oder zur gewünschten Tat zwingen. Dieser Definition fehlen allerdings, dem Autor aus [16] zufolge, die physischen Effekte, die Cyber-Terrorismus verursacht, sowie eine klare Unterscheidung zu dem Begriff Hacktivismus. [19] im Vergleich dazu sieht unter anderem die Verwendung von Computer-Netzwerk-Tools zum Abschalten national kritischer Infrastrukturen (zum Beispiel Infrastrukturen von Energieversorgern, Transportunternehmen und Regierungen) als Cyber-Terrorismus an. Die Definition aus [19] bewertet der Autor aus [16] als unpräzise, da dann auch Mitarbeiterinnen und Mitarbeiter von Unternehmen, die kritische Infrastruktur betreiben, als Cyber-Terroristinnen und Cyber-Terroristen gelten, wenn sie im Zuge von technischen oder sicherheitsrelevanten Gründen die Infrastruktur abschalten. Zusätzlich wird laut [16] in der Definition aus [19] nicht in Hacktivisten und Cyber-Terroristen unterschieden.

Die resultierende Definition von Cyber-Terrorismus aus [16] lautet schlussendlich „The use, making preparations for, or threat of action designed to cause a social order change, to create a climate of fear or intimidation amongst (part of) the general public, or to influence political decision-making by the government or an international governmental organisation; made for the purposes of advancing a political, religious, racial, or ideological cause; by affecting the integrity, confidentiality, and/or availability of information, information systems and networks, or by unauthorised actions affecting information and communication technology-based control of real-world physical processes; and it involves or causes:

- violence to, suffering of, serious injuries to, or death of (a) person(s)
- serious damage to property
- a serious risk to health and safety of the public
- a serious economic loss
- a serious breach of ecological safety
- a serious breach of the social and political stability and cohesion of a nation. “ [16][1]

[1] Zu Deutsch: Die Verwendung, Vorbereitung oder Androhung von Handlungen, die darauf abzielen, einen gesellschaftlichen Ordnungswandel herbeizuführen, ein Klima der Angst oder Einschüchterung in der (Teil-)Öffentlichkeit zu schaffen oder politische Entscheidungen durch die Regierung oder eine internationale Regierungsorganisation zu beeinflussen, die zum Zwecke der Förderung einer politischen, religiösen, rassischen oder ideologischen Sache, durch Beeinträchtigung der Integrität, Vertraulichkeit und/oder Verfügbarkeit von Informationen, Informationssystemen und -netzwerken oder durch unbefugte Handlungen, die die informations- und kommunikationstechnische Kontrolle realer physischer Prozesse betreffen, durchgeführt werden; und sie beinhalten oder verursachen:
Gewalt gegen, Leiden, schwere Verletzungen oder Tod von (einer) Person(en)

- Gewalt gegen, Leiden, schwere Verletzungen oder Tod von (einer) Person(en)
- schwere Sachschäden
- ein ernsthaftes Risiko für die Gesundheit und Sicherheit der Bevölkerung

Die sehr spezielle Definition aus [16] schränkt aufgrund ihrer Genauigkeit die Anzahl der Fälle, die Cyber-Terrorismus zuzuschreiben sind, sehr stark ein und auch der Autor selbst kommt zu dem Schluss, dass es nach seiner Definition nicht sehr viele Fälle gibt, die unter den Begriff Cyber-Terrorismus fallen. Daher soll für diese Arbeit die Definition für den Begriff Cyber-Terrorismus etwas abgeschwächt werden und stattdessen Fälle betrachtet werden, die eines oder mehrere der folgenden Merkmale aufweisen:

- Das Ziel des Cyber-Angriffs ist keine einzelne Person, ausgenommen einflussreiche Personen, wie beispielsweise Religionsoberhäupter, Staats- und Regierungschefs, sondern die Bevölkerung und/oder die Regierung eines Landes
- Die betroffene Regierung und/oder das Volk wird eingeschüchtert und/oder zu Handlungen gezwungen, die sie aufgrund des Angriffs durchführen
- Dem Angriff folgen schwere Einschränkungen des öffentlichen Lebens
- Die Angreiferinnen und/oder Angreifer sind politisch/ideologisch motiviert
- Gewalt wird seitens der Angreiferinnen und/oder Angreifer nicht ausgeschlossen
- Mit überwiegender Wahrscheinlichkeit wurde der Angriff von einer Gruppierung durchgeführt, welche laut [7] oder [8] als terroristische Vereinigung geführt wird. Als Referenzdatum zu den Listen gilt hier der Stand vom 8. Juli 2019

Nachdem es nicht möglich ist sämtliche Cyberangriffe zu untersuchen, sollen nur neun Fälle ausgewählt werden. Daher wird eine Priorisierung durchgeführt, welche Fälle mit mehreren Merkmalen bevorzugt. Grundsätzlich gilt für die Auswahl, dass Cyber-Terrorismus das illegale Handeln von einzelnen Individuen oder einer Gruppe über das Medium Internet, die mit ihren Handlungen eine gewaltsame Veränderung im Sinne ihrer Vorstellungen bewirken möchte, beinhaltet. An dieser Stelle ist ebenfalls anzumerken, dass beim Cyber Terrorismus Computertechnologie sowohl die Waffe als auch das Ziel ist [20].

1.3. Unterschied zu Cyber-Warfare

Neben dem Begriff des „Cyber-Terrorismus“ gibt es zum Beispiel den Begriff „Cyber-Warfare“. Warfare kann zu Deutsch auf Kriegsführung übersetzt werden. Die Bedeutung des Wortes Cyber wurde bereits genauer erläutert. Dieser Definition ist nun die Bedeutung des Wortes Kriegsführung hinzuzufügen. Laut [21] bezeichnet das Wort „Krieg“ einen „mit Waffengewalt ausgetragener Konflikt zwischen Staaten, Völkern“ [21] und weiter eine „größere militärische Auseinandersetzung, die sich über einen längeren Zeitraum erstreckt“ [21]. Da Cyber-Warfare im Cyberraum stattfindet ist die hier angewandte Waffengewalt ähnlich zum Cyber-Terrorismus zu betrachten, also Waffe und Ziel sind Computertechnologie. Aus der Definition des Wortes „Krieg“ geht noch hervor, dass es sich um einen Konflikt zwischen Staaten handelt, was beim Cyber-Terrorismus nicht der Fall sein muss.

Genauere Definitionen zum Wort „Cyber-Warfare“ finden sich in [22] wieder. Die Autoren vergleichen einige bestehende Definitionen von Cyber-Warfare und bilden daraus eine eigene Version. Zusätzlich wird anhand der erstellten Definition ein Modell entwickelt, welches dabei helfen soll je nach Akteurin oder Akteur und ihren beziehungsweise seinen Intentionen festzustellen, ob es sich um Cyber-Warfare handelt oder ob der Fall in eine andere Kategorie gehört. Die Grenzen zwischen Cyber-Terrorismus und Cyber-Warfare sind allerdings nicht klar auszulegen, da sowohl Merkmale von Cyber-Terrorismus bei Cyber-Warfare auftreten können und umgekehrt.

- ein schwerer wirtschaftlicher Verlust
- eine schwerwiegende Verletzung der ökologischen Sicherheit
- eine schwerwiegende Verletzung der sozialen und politischen Stabilität und des Zusammenhalts einer Nation

1.4. Unterschied zu „Hacktivismus“

Das Wort Hacktivismus setzt sich aus den zwei Wörtern Hacking und „Aktivismus“ zusammen [23]. Hacktivismus ist laut [13] und [14] auf dem Vormarsch und findet mehr und mehr Anhängerinnen und Anhänger. Eine bekannte Hacktivisten Gruppe ist laut [13] „Anonymous“, die vor allem dadurch bekannt ist, da sehr oft in den Nachrichten über ihre Aktionen berichtet wurde. Weitere Informationen zum Thema Aktivismus und dem Unterschied zu Hacktivismus finden sich in [14].

Die Ziele von Hacktivismus sind laut [23] ähnlich zu denen einer Cyber-Terroristin oder denen eines Cyber-Terroristen. Die Autorin aus [23] beschreibt, dass auch Hacktivistinnen und Hacktivisten ideologisch motiviert sind, so wie Cyber-Terroristinnen und Cyber-Terroristen. Auch die Angriffstypen sind ähnlich, da oft Denial of Service Attacken und Datenmanipulationen durchgeführt werden.

Die Unterschiede zwischen Hacktivismus und Cyber-Terrorismus liegen laut [20] darin, dass Angriffe, die unter Cyber-Terrorismus fallen, „computergeneriert, politisch motiviert, gewaltsam und psychologisch nötigend“ sind. Ähnlich zu Cyber Warfare sind auch die Grenzen zwischen Cyber-Terrorismus und Hacktivismus nicht klar, da die Merkmale von Cyber-Terrorismus auch Merkmale von Hacktivismus sind und umgekehrt.

Die wesentlichen Merkmale der drei Begriffe Cyber-Terrorismus, Cyber-Warfare und Hacktivismus sind in Tabelle 1: Kurzübersicht Begriffe zusammengefasst. Es wurden die Kategorien Akteur/Akteurin, Finanzierung, Motivation, Ziele und Methoden für die drei Begriffe unterschieden. Die Akteurin oder der Akteur kann entweder ein Staat sein, der seine Interessen vertritt oder eine Privatperson ohne staatlichen Akteur im Hintergrund. Die Finanzierung der Akteurinnen und Akteure kann durch Privatvermögen der handelnden Terroristinnen und Terroristen oder Hacktivistinnen und Hacktivisten geschehen, aber auch durch Spenden von anderen Interessensvertreterinnen und Interessensvertretern, die sich nicht aktiv an den Aktionen beteiligen. Staaten finanzieren Kriegsführung durch das eigene Budget. Schwieriger ist es bei der Motivation, da diese sehr nahe beieinanderliegen und auf Meinungsverschiedenheiten beruhen (vergleiche mit den Erläuterungen aus Kapitel 1.3 und 1.4). Auch die Ziele sind sehr ähnlich, da Terroristinnen beziehungsweise Terroristen und Hacktivistinnen und Hacktivisten Regierungen und Unternehmen als Angriffsziel auswählen können. Nur Cyber-Warfare schränkt sich ausschließlich auf Konflikte zwischen Staaten ein. Terroristinnen und Terroristen schrecken vor Gewalt nicht zurück und setzen auf psychologische Nötigung. Gewaltsam sind Kriege zwischen Staaten auch, während Hacktivistinnen und Hacktivisten friedliche Absichten verfolgen.

Begriff	Akteur/Akteurin	Finanzierung	Motivation	Ziele	Methoden
Cyber-Terrorismus	Privatpersonen	Privatvermögen, Diebstahl, Spenden	Ideologie, Politik,	Regierungen, Unternehmen	Gewalt, Psychologie
Cyber-Warfare	Staaten	Staatsvermögen	Politik	Regierungen	Gewalt
Hacktivismus	Privatpersonen	Privatvermögen, Spenden	Ideologie	Regierungen, Unternehmen	Friedlich

Tabelle 1: Kurzübersicht Begriffe[2]

1.5. Aufbau der Arbeit

In Kapitel 2 wird auf ähnliche Arbeiten eingegangen, die bereits rund um das Thema Cyber-Terrorismus existieren. Im nächsten Kapitel werden einige ausgewählte Fälle von Cyber-Terrorismus präsentiert. Die Fälle werden aufbereitet und genauer analysiert, um anschließend in 4. neben einer Zusammenfassung Parallelen und Unterschiede herauszuarbeiten. Des Weiteren wird in 5. näher darauf eingegangen, welche Techniken zur Prävention sich aus den Fällen von Kapitel 3.ableiten lassen. Abschließend wird in 6. ein kurzer Ergebnisrückblick gegeben und ein Ausblick auf die Zukunft von Cyber-Terrorismus.

[2] Die Ableitung der Tabelle erfolgt hauptsächlich auf Basis der Erkenntnisse aus Kapitel 1.2 – 1.4. Zusätzliche Informationen wurden aus den gewonnenen Erkenntnissen verschiedener Quellen abgeleitet. Dazu gehören Informationen der Spalten Akteure, Finanzierung und Ziele. Akteure und Ziele ergeben sich aus den beschriebenen Fällen in Kapitel 3. Die Finanzierung wurde von [53] und [136] abgeleitet.

2. Verwandte Arbeiten

Das Ziel dieser Literaturrecherche ist es, die neuen Angriffsmethoden und Möglichkeiten, die sich für Terroristinnen und Terroristen im Cyberspace anbieten, etwas näher zu betrachten beziehungsweise darauf aufmerksam zu machen, dass sie bereits genutzt werden und ein Problem darstellen. Außerdem soll sie weiterführende Informationen rund um das Thema Cyber-Terrorismus bieten. Zusätzlich sollen Ergebnisse bereits existierender Arbeiten auf diesem Gebiet später mit den Ergebnissen dieser Arbeit verglichen werden können.

2.1. Herkömmlicher Terrorismus und Cyber-Terrorismus

Terrorismus existierte schon in einer Zeit, bevor es eine weltweite Vernetzung durch das Internet gab [24]. Laut [24] basierte die soziale Vernetzung damals auf Schlüsselorten, wie Schulen, Marktplätzen und religiösen Einrichtungen. [24] sieht die Anschläge vom 11. September 2001 als Ursache dafür, dass terroristische Organisationen ihre Aktivitäten in den Cyberspace verlagert haben, da geheime Treffpunkte, Gasthäuser, extremistische Moscheen und festinstallierte Trainingscamps zunehmend in das Visier von Anti-Terror-Einheiten gerieten und damit nicht mehr sicher waren.

Terrorismus in der analogen Welt, abseits der Cyber-Welt, verfolgt zwar die gleichen Ziele (siehe Kapitel 1.1. Begriffserklärungen), aber es gibt dennoch Unterschiede in der Arbeitsweise. Neben Gruppierungen, die rein im Internet aktiv sind, gibt es auch Gruppierungen, die es nur zur Kommunikation und Koordination nutzen [25]. Die Grenze hierbei ist allerdings nicht klar zu definieren und sie verschwimmt immer mehr [25]. Trotz der Attraktivität, welche durch die zahlreichen Möglichkeiten im Cyberspace herrscht, soll das aber nicht heißen, dass jede Terrorgruppe im Internet unbedingt aktiv werden muss.

Ansätze für die Unterschiede zwischen herkömmlichem Terrorismus und Cyber-Terrorismus finden sich unter anderem in [26]. Hier wird zum Beispiel beschrieben, dass eine herkömmliche Terroristin oder ein herkömmlicher Terrorist ein Ziel aussucht, das physisch abgegrenzt ist und daher nur Einfluss auf die nahe Umgebung hat. Diese Grenzen verschwinden laut [26] jedoch im Cyberspace, da alles miteinander über das Internet verbunden ist und es diese Einschränkung nicht mehr gibt.

Welche Ursachen extremistische Vereinigungen dazu bewegen ihre Aktivitäten in den Cyberspace zu verlegen oder zu erweitern untersuchen die Autoren in [27]. Im Zuge dessen wurden unterschiedliche Gruppen von Expertinnen und Experten zu ihrer Meinung bezüglich dessen befragt, welche Eigenschaften extremistische Gruppierungen aufweisen, damit sie Aktivitäten im Cyberspace durchführen. Die Expertinnen und Experten stammen aus unterschiedlichen Bereichen, nämlich folgenden:

- öffentlicher Bereich
- privater Bereich
- akademischer Bereich (Fokus auf Cyber Security)

Zusätzlich wurde darauf geachtet, dass in diesen Gruppen Personen mit und ohne technischen Hintergrund teilnehmen. Die Personen aus der Gruppe mit technischem Hintergrund kommen aus Bereichen wie „computer science or computer engineering“[3] [27], jene Personen ohne technischem Hintergrund arbeiten beispielsweise als „policy makers, policy analysts, and academics“[4] [27]. Ziel war einerseits zu untersuchen, bei welchen Merkmalen diese Gesamtgruppe an Expertinnen und Experten extremistischen Vereinigungen Cyber-Aktivitäten zuschreiben. Andererseits wurden auch die Unterschiede zwischen den Bereichen (Anmerkung: öffentlich, privat und akademisch) und den Gruppen mit und ohne technischem Hintergrund untersucht.

Den Studienteilnehmerinnen und Studienteilnehmern aus [27] wurden die in Tabelle 2: Merkmale der Studie aus [27] gelisteten 22 Merkmale vorgelegt, die dazu führen, dass eine extremistische Vereinigung im Cyberspace

[3] Zu Deutsch in etwa: Computerwissenschaften oder Computertechnik

[4] Zu Deutsch in etwa: Verfasser und Analysten von Richtlinien, sowie Akademiker

aktiv wird. Aus diesen wählten sie die ihrer Meinung nach fünf ausschlaggebendsten Merkmale aus. Anschließend sollten diese fünf Merkmale noch nach Einflussgröße gereiht werden. Tabelle 2 enthält neben den originalen englischen Begriffen aus [27] auch eine deutsche Übersetzung der Begriffe. Die Autoren werteten die Ergebnisse statistisch genau aus. Ein wesentlicher Überblick findet sich in Tabelle 3: Ergebnisüberblick aus [27]. In manchen Fällen gab es in den Gruppierungen die gleiche Anzahl an Nennungen für unterschiedliche Begriffe. In diesem Fall werden diese zwei Eigenschaften gleich gewertet. In Tabelle 3 wird dies durch einen fehlenden Trennstrich zwischen Wertungen und ein verbindendes „*und*" gekennzeichnet.

Englischer Originalbegriff aus [27]	**Deutsche Übersetzung**
Prior Terrorist Activities	Frühere terroristische Aktivitäten
Propensity for Violence	Gewaltbereitschaft
Prior Illicit Activities	Frühere illegale Aktivitäten
Observed Internet Sophistication	Beobachtete Internet Erfahrung
Level of Internet Presence	Stärke der Internetpräsenz
Prior Cyber-Attack	Vorheriger Cyber-Angriff
Penchant for Innovation	Neigung zu Innovation
Tactical Sophistication	Taktische Erfahrung
Technical Sophistication	Technische Erfahrung
Ideology	Ideologie
Access to Human Resources	Zugang zu Personenressourcen
Network Access	Netzwerkzugriff
Human Resources Available	Verfügbare Personenressourcen
Financial Resource	Finanzielle Mittel
Membership Distortion	Einstellung der Mitglieder
Member Composition	Zusammensetzung der Mitglieder
Leadership Fractionalization	Aufteilung der Führung
Leadership Distortion	Verzerrung durch die Führung
Leadership	Führung
Organizational Cohesion	Zusammensetzung der Vereinigung
Organizational Structure	Struktur der Vereinigung
Organization Size	Größe der Vereinigung

Tabelle 2: Merkmale der Studie aus [27]

<table>
<tr><th></th><th colspan="6">Teilnehmerinnen/Teilnehmer</th></tr>
<tr><th>Wertung</th><th>Alle</th><th>Technischer Hintergrund</th><th>Kein technischer Hintergrund</th><th>Öffentlicher Bereich</th><th>Privater Bereich</th><th>Akademischer Bereich</th></tr>
<tr><td>1</td><td>Stärke der Internet-präsenz</td><td rowspan="2">Stärke der Internetprä-senz und Zugang zu Personen-ressourcen</td><td>Stärke der Internetpräsenz</td><td>Stärke der Internetprä-senz</td><td rowspan="2">Netzwerkzu-griff und Ideologie</td><td>Aufteilung der Führung</td></tr>
<tr><td>2</td><td>Führung</td><td>Neigung zu Innovation</td><td>Zugang zu Personen-ressourcen</td><td rowspan="3">Führung und Zusammen-setzung der Vereinigung und Zusammen-setzung der Mitglieder und Gewaltbe-reitschaft</td></tr>
<tr><td>3</td><td>Zugang zu Personen-ressourcen</td><td>Finanzielle Mittel</td><td>Führung</td><td>Finanzielle Mittel</td><td rowspan="3">Stärke der Internetprä-senz und Neigung zu Innovation und Führung</td></tr>
<tr><td>4</td><td>Neigung zu Innovation</td><td rowspan="2">Führung und Verfügbare Personen-ressourcen</td><td>Gewaltbereit-schaft</td><td>Beobachtete Internet Erfahrung</td></tr>
<tr><td>5</td><td>Verfügbare Personen-ressourcen</td><td>Verfügbare Personen-ressourcen</td><td>Technische Erfahrung</td></tr>
</table>

Tabelle 3: Ergebnisüberblick aus [27]

Im Wesentlichen kommen die Autoren aus [27] zu dem Schluss, dass die drei einflussreichsten Eigenschaften, die die Expertinnen und Experten genannt haben, „Stärke der Internetpräsenz“, „Zugang zu Personenressourcen“ und „verfügbare Personenressourcen“ sind. Im Vergleich dazu wurden im Zuge der Umfrage von [27] Eigenschaften wie „Frühere terroristische Aktivitäten“, „Frühere illegale Aktivitäten“, „Vorheriger Cyber-Angriff“, „Taktische Erfahrung“, „Einstellung der Mitglieder“, „Verzerrung durch die Führung“, „Struktur der Vereinigung“ und „Größe der Vereinigung“ sehr selten genannt und scheinen in Tabelle 3 gar nicht auf. Allgemein gesehen sind die von den Expertinnen und Experten in [27] genannten Eigenschaften Großteils Merkmale, die prinzipiell benötigt werden, um überhaupt Cyber Angriffe durchzuführen. Anders ausgedrückt, wenn Mittel wie ein „Netzwerkzugriff“ und „Finanzielle Mittel“ vorhanden sind und auf Voraussetzungen wie „Verfügbare Personenressourcen“, „Zugang zu Personenressourcen“, „Technische Erfahrung“ und eine gewisse Affinität für Technik stoßen, dann kann man laut [27] davon ausgehen, dass die betroffenen Vereinigungen Cyber-Angriffe durchführen werden.

Die ersten Webseiten mit terroristischen Inhalten gab es in den späten 1990er Jahren [28]. Terroristinnen und Terroristen nutzen das Internet für psychologische Kriegsführung, Propagandazwecke wie Spendensammlung, Rekrutierung, Data Mining und Koordination von Aktionen [29]. Während Terroristinnen und Terroristen aber nicht immer nur auf die öffentlichen sichtbaren Teile des Internets zugreifen und diese für ihre Zwecke missbrauchen, werden sie auch zunehmend im Deep Web aktiv [29]. Das Deep Web ist jener Teil des Internets, der nicht öffentlich sichtbar ist [30]. Laut [30] befinden sich etwa 4% des Inhalts im öffentlich sichtbaren Bereich, der von Suchmaschinen indiziert wird, und die restlichen 96% im Deep Web. Der Zugriff auf das Deep Web ist nicht sehr schwierig und erfordert im Grunde genommen nur den Tor Browser [30] [31]. Terroristinnen und Terroristen können daher sehr leicht im Deep Web aktiv werden, wenn sie bereits Zugriff auf das normale Internet haben. Anleitungen, sowie zusätzliche Tipps, wie man anonym bleibt sind ebenfalls leicht zu finden [30] und machen es dadurch schwerer die Terroristinnen und Terroristen zurückzuverfolgen. Terroristinnen und Terroristen nutzen das Deep Web vorwiegend zur verschlüsselten Kommunikation, zum Datenaustausch, zum Wissensaustausch, zur Rekrutierung, sowie zur Planung und Koordination [32].

Schließlich bleibt noch die Frage offen, wo geografisch gesehen terroristische Gruppierungen aktiv werden. Viele Aktivitäten gehen zunächst von terroristischen Organisationen aus dem Nahen Osten in der Region um Syrien und dem Irak aus [7]. Es wurden bereits einige Daten zu den Inhalten von Terroristinnen und Terroristen aus dieser Region im Internet gesammelt und zur Verfügung gestellt [33] [34]. Allerdings gibt es auch in Südostasien terroristische Vereinigungen, die das Internet für ihre Zwecke nutzen [35]. Hier werden Manifeste mit extremistischen Inhalten und Propaganda veröffentlicht [35]. Des Weiteren wird versucht neue Mitglieder zu rekrutieren und es wurden auch Beweise für Kommunikation zwischen Mitgliedern gefunden [35]. Einen guten Überblick über die 10 tödlichsten Terrorgruppierungen (nicht ausschließlich Cyber-Terroristen) weltweit bietet Abbildung 1: Tödlichste Terrorgruppen und ihre Hauptquartiere [36]. Darin sind Anschläge mit mehr als 100 Toten im Zeitraum zwischen 2000 und November 2015, sowie die Heimatländer der Terrorgruppen zu sehen.

Abbildung 1: Tödlichste Terrorgruppen und ihre Hauptquartiere [36]

2.2. Cyber-Terrorismus in sozialen Netzwerken

Bereits in [15] wird erwähnt, dass Terroristinnen und Terroristen in Gruppierungen arbeiten. Mehrere Personen mit unterschiedlichen Stärken können den Erfolg von Terror erhöhen. Für eine Gruppe von Terroristinnen und Terroristen kann es daher nicht schaden neue Anhänger für ihre Ideologie zu finden. Dafür muss die Gruppe auf sich aufmerksam machen.

Es gibt bereits Arbeiten, die sich mit dem Thema Propaganda für terroristische Zwecke beschäftigen. In [37] zum Beispiel beschreibt der Autor, wie der „Islamische Staat“ (Anmerkung: Eine terroristische Vereinigung) soziale Plattformen, wie zum Beispiel YouTube, Facebook und Twitter nutzt, um Angehörige der islamischen Glaubensrichtung für ihre Zwecke anzuwerben. Des Weiteren nutzt er laut [37] das Internet neben der Verbreitung von Propaganda für Spendensammlungen, Rekrutierung, Informationsaustausch, Planung und psychologische Kriegsführung. Letzteres beschreiben zum Beispiel die Autoren in [38] nochmals genauer.

In [39] kommt der Autor zu dem Schluss, dass bereits sehr viele Videos mit terroristischer Propaganda auf der Videoplattform „YouTube“ existieren und, dass immer noch Videos hochgeladen werden. Eine Zensur ist laut [39] aber nicht so leicht möglich, da diese leicht umgangen werden kann. Der Autor in [40] beschäftigt sich in seiner Arbeit damit, inwiefern die Kontrolle von hochgeladenen Inhalten von Menschen und Maschinen durchgeführt werden. Jedenfalls arbeiten Betreiber von Plattformen sozialer Medien, wie „Facebook“, daran terroristische Inhalte zu entfernen [3].

Es existieren bereits Ansätze für das Erkennen von Cyber-Terrorismus und Extremismus in Texten und es gibt Algorithmen, die darauf trainiert werden, automatisiert Texte zu durchsuchen und entsprechende Inhalte auszumachen [41]. Die Autoren aus [41] nutzen dabei Datensets, die antisoziales Verhalten wiederspiegeln. Genauer ausgedrückt handelt es sich um ein Datenset, das in der Arbeit von [42] zusammengestellt wurde und „aggressive, gewalttätige und feindliche Texte“ [42] enthält. Quelle für dieses Datenset aus [42] sind Blog-Posts und News-Webseiten. Bei den Texten selbst handelt es sich inhaltlich gesehen um Manifeste von Serienkillerinnen und Serienkillern, antisozialen Texten, Terrorismus, gewaltbasierten Texten und Abschiedsbriefen [42]. Dieses Datenset enthält die positiv gekennzeichneten Texte bezüglich Terrorismus auf denen die Ergebnisse von [41] basieren. Für die negativen Datensätze, also ohne terroristischen Inhalten, wurde in [41] ein Datenset mit Filmkritiken, bestehend aus sowohl positiven als auch negativen Kritiken, verwendet [43]. Für die Experimente in [41] wurden 48 Einträge aus [42] und 480 Einträge aus [43] verwendet. Die Autoren aus [41] verglichen mehrere Methoden mit unterschiedlichen Klassifizierungen, was zu Erkennungsgenauigkeiten von bis zu ungefähr 99% führte.

Die Autoren aus [44] gehen noch einen Schritt weiter und untersuchen sehr speziell, wie man Radikalisierung von anderen Nutzerinnen und Nutzern in Social Media Plattformen erkennen kann. Im Zuge der Arbeiten wurden die Tweets von Nutzerinnen und Nutzern auf Twitter untersucht. Man stützt sich auf die Ergebnisse anderer Forschungen ([45] [46] [47] [48]), die zu dem Schluss gekommen sind, dass für eine erfolgreiche Radikalisierung eine bestimmte Terminologie und Sprache genutzt wird. Deshalb wurden nicht einfach wie bei [41] terroristische Inhalte mit „normalen“ Texten verglichen, sondern Tweets, die zwar die gleichen Begrifflichkeiten verwenden, aber unterschiedlich einsetzen. Anders ausgedrückt kann eine Person, die sich für den islamischen Staat einsetzt und dafür werben möchte, Wörter wie „ISIS“, „Kalifat“ und/oder „Dschihad“ anders in Verbindung bringen als beispielsweise ein Nachrichtensender, der eine Berichterstattung auf rein sachlicher Ebene vermitteln möchte. Das verwendete Datenset für die positiven, also radikalisierenden Tweets, ist ein Datenset bestehend aus 17.350 Tweets von 112 unterschiedlichen Nutzerinnen und Nutzern, welches unter [33] verfügbar ist. Das verwendete Datenset für nicht pro islamischen Staat radikalisierenden Tweets stammt von [34]. Die Autoren geben außerdem an, dass einige der Konten, von denen die Tweets stammen, seit der Erhebung gesperrt beziehungsweise geblockt wurden. Es wurde daher seitens [44] darauf geachtet zum Zeitpunkt der Arbeiten nur Tweets jener Accounts zu verwenden, die nicht gesperrt beziehungsweise geblockt sind. Mit den durchgeführten Methoden zur Erkennung einer Radikalisierung konnte ein Bestwert von 90,6% korrekter Klassifizierung erreicht werden [44].

Ein weiterer Schritt in der Vermeidung von Online Propaganda und Terrorismus ist es zu verstehen, wann beziehungsweise wie aktiv die Unterstützerinnen und Unterstützer von Terrorgruppen in Sozialen Medien sind und was sie senden. Mit diesem Thema beschäftigen sich die Autoren aus [49]. Ferner fokussierte man sich darauf, wie aktiv Unterstützerinnen und Unterstützer des Islamischen Staates auf Twitter sind und welche Informationen sie verbreiten. Die Analysen basieren auf zwei Datensätzen, wobei einerseits wie schon von [44]

der Datensatz von Kaggle [33] und andererseits ein selbst gesammelter Datensatz zum Einsatz kamen. Für die Forschung wurden bezüglich der Tweets aus [33] hauptsächlich jene aus dem Jahr 2016 genutzt, der eigens gesammelte Datensatz enthält Großteils Tweets aus dem Jahr 2017.

Zum einen wurden die Twitter-Aktivitäten mit Terror-Ereignissen, die 2016 und 2017 stattfanden, verglichen und zum anderen untersucht, was von den Nutzerinnen und Nutzern getwittert wurde. Für den eigenständig gesammelten Datensatz wurden Tweets, die die Wörter „Syria“ oder „ISIS“ (Islamischer Staat im Irak und in Syrien) enthielten, gesammelt. Außerdem wählte man Nutzer mit einschlägigen Bildern (Fahnen des Islamischen Staates, Personen mit Waffen) und Nachrichten. Daraus ergab sich ein Datenset mit 18000 Tweets, 50 Nutzerinnen beziehungsweise Nutzern und 2000 Followern. In Tabelle 4: Vergleich der Datensätze ist ein kurzer Vergleich der beiden Datensätze, die in [49] verwendet wurden, ersichtlich.

Ein Ergebnis der Studie ist der Vergleich von gesendeten Tweets zu terroristischen Ereignissen. Darin ist zu sehen, dass bei den untersuchten Profilen die Anzahl der Pro Islamischem Staat abgesetzten Tweets zunimmt, wenn sich die Terrororganisation zu einem erfolgten Anschlag bekannt hat. Diese Zusammenhänge können in Abbildung 2: Twitter Aktivitäten nach [33], welche den Kaggle Datensatz [33] widerspiegelt, und Abbildung 3: Twitter Aktivitäten nach [49], welche den von [49] eigenständig gesammelten Datensatz zeigt, sowie der dazugehörigen Liste mit Ereignissen in Tabelle 5: Auszug aus [49] über Terroranschläge von Jänner 2016 bis April 2017, nachgesehen werden. Zusätzlich wurde analysiert, welchen Wortschatz die Unterstützerinnen und Unterstützer der Terrormiliz Islamischer Staat nutzen. Im Zuge dessen entstanden 4 Wortwolken (siehe Abbildung 4: Wortwolken [49]), die das verwendete Vokabular deutlich machen. Bei diesen Wortwolken merken die Autoren an, dass Stoppwörter entfernt wurden. Während im Kaggle-Datensatz [33] die Worte „ISIS“ und „Syria“ eindeutig, sowohl allgemein als auch bei den Hashtags, dominieren gibt es beim eigenen Datensatz größere Unterschiede. Allgemein dominiert hier „god“ und auch „allah“, in der Hashtag Wolke allerdings eher Schauplätze wie „Mosul“, „Syria“, „Hama“, „Sinai“ und allen voran „Urgent“.

Die Ursachen, warum sich Menschen überhaupt von terroristischen Organisationen, wie dem islamischen Staat radikalisieren lassen erläutert der Autor aus [50]. Er beschreibt in seiner Arbeit mehrere Stufen, die eine Person durchläuft, während sie radikalisiert wird [50]. Im Wesentlichen werden in [50] als Gründe für eine Radikalisierung fehlende Integration in die Gesellschaft, Armut und Diskriminierung erwähnt. Geisteskrankheit ist eher selten ein Grund, weshalb Menschen zu Terroristen werden und es gibt auch eher selten Terroristinnen und Terroristen, die psychisch krank oder verrückt sind [51].

	Gesammelt von Kaggle [33]	**Gesammelt von** [49]
Jahre	Jänner 2015 bis Mai 2016	Februar 2017 bis April 2017
Anzahl der Tweets	17.350	18.000
Benutzer	112	50
Einflüsse auf die Auswahl	Texte + Bilder	Texte + Bilder + Zufall
Eigenschaften der Statistiker	Experten für Terrorismus	Keine terroristische Expertise

Tabelle 4: Vergleich der Datensätze

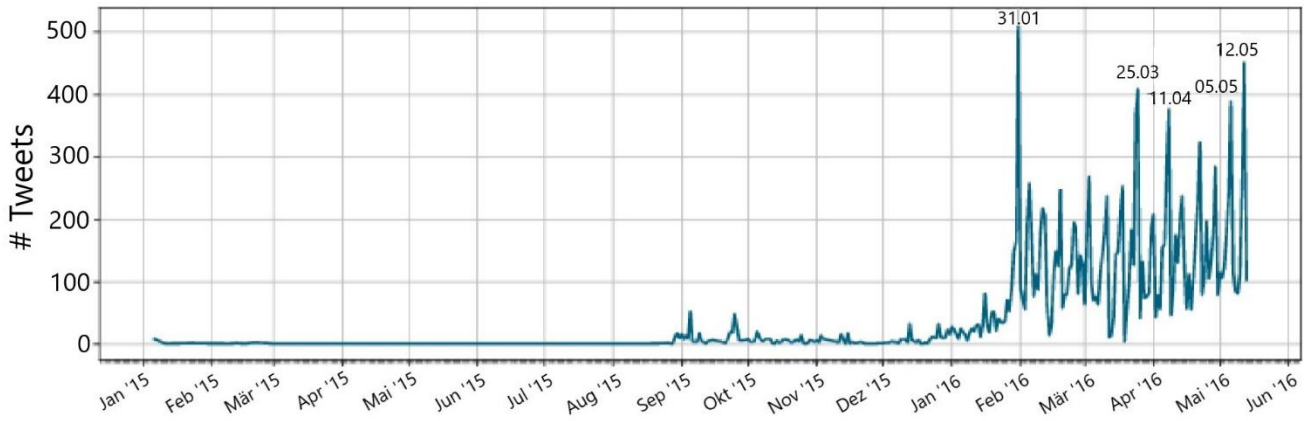


Abbildung 2: Twitter Aktivitäten nach [33]

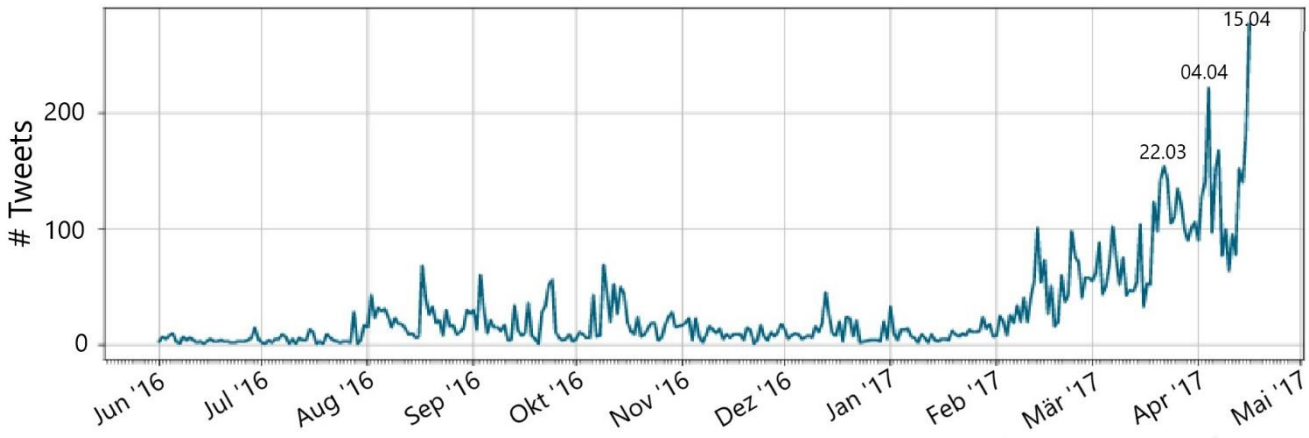


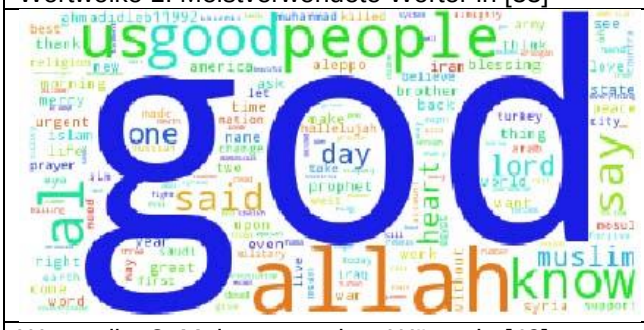
Abbildung 3: Twitter Aktivitäten nach [49]

Datum	Ort	Verletzt und getötet	Täter
31.01.2016	Irak	160	Islamischer Staat
25.03.2016	Irak	106	Islamischer Staat
08.04.2016	Irak	475	Islamischer Staat
05.05.2016	Irak	129	Islamischer Staat
11.05.2016	Irak	302	Islamischer Staat
22.03.2017	Vereinigtes Königreich	65	Islamischer Staat
04.04.2017	Syrien	170+	Islamischer Staat
15.04.2017	Syrien	226	Islamischer Staat

Tabelle 5: Auszug aus [49] über Terroranschläge von Jänner 2016 bis April 2017

Wortwolke 1: Meistverwendete Wörter in [33]

Wortwolke 2: Hashtagnutzung in [33]



Wortwolke 3: Meistverwendete Wörter in [49]

Wortwolke 4: Hashtagnutzung in [49]

Abbildung 4: Wortwolken [49]

2.3. Finanzierung von Terrorismus

Sowohl für herkömmlichen Terrorismus als auch für Cyber-Terrorismus kann es sein, dass finanzielle Mittel gebraucht werden, damit die Ziele erreicht werden. Kosten können zum Beispiel durch die Ausbildung einzelner Personen entstehen, wenn diese erst die nötigen Fähigkeiten erlernen müssen, die sie zur Durchführung ihrer Angriffe benötigen. Für Cyber-Terrorismus ist technisches Verständnis in der Cyber Welt von Vorteil, weshalb eine zusätzliche technische Ausbildung die Wahrscheinlichkeit für einen erfolgreichen Angriff erhöhen kann. In jedem Fall ist ein internetfähiges Gerät für Cyber-Terrorismus unumgänglich, da ansonsten dem Cyber-Terroristen die „Waffe" für seinen Angriff fehlt. Für diese anfallenden Kosten braucht es Wege zur Finanzierung. Die folgenden Erläuterungen sollen nur beispielhaft Wege der Finanzierung für Terrorismus über das Internet und mit Computertechnologie demonstrieren und sind nicht als ausschließliche Methoden, über die sich terroristische Vereinigungen finanzieren, zu verstehen.

Younis Tsouli, auch bekannt unter dem Namen „irhabi007"[5], arbeitete eine Zeit lang für die Terrororganisation Al-Qaida[6] [52]. Er kämpfte jedoch nie und führte keine physischen Angriffe in der realen Welt aus. Stattdessen agierte er im Cyberspace, wo er Webseiten und Video-Plattformen einrichtete, die pro Al-Quaida Inhalte verbreiteten und sich negativ gegenüber den Vereinigten Staaten und Großbritannien verhielten [52]. Younis Tsouli selbst agierte gemeinsam mit zwei Mitstreitern, nämlich Waseem Mughal und Tariq al-Daour [53], von seiner Wohnung in London aus [52] und nutzte zunächst nur kostenfreie Webhosting-Plattformen um die Inhalte, die er von der Al-Quaida erhielt, veröffentlichen zu können. Da die gratis Webplattformen jedoch nur begrenzte Bandbreiten zur Verfügung stellten, verlangsamten sie Tsouli bei seinen Aktivitäten [54]. Dies führte dazu, dass er zu Seiten mit besseren Kapazitäten wechselte, wodurch aber auch Kosten auf ihn zukamen [54].

Um diese Kosten zu decken begann das Trio um Tsouli Kreditkartennummern zu stehlen. Für die Finanzierung war Tariq al-Daour zuständig, welcher die Informationen von 37 000 Kreditkarten in seinem Apartment hortete. Der Diebstahl der Informationen erfolgte online durch Phishing und die Verbreitung von Trojanern. Insgesamt wurden so mehr als 3,5 Millionen $ gestohlen. Einen Teil des erbeuteten Geldes, sowie Teile der gestohlenen Informationen von den rechtmäßigen Inhabern, nutzte Tsouli um mehr als 180 Website-Domänen bei 95 verschiedenen Web-Hosting Firmen in den Vereinigten Staaten und Europa zu registrieren. Es konnte genug Geld erwirtschaftet werden, sodass Mughal und al-Daour nicht nur Tsoulis Aktivitäten unterstützen konnten, sondern selbst Einkaufslisten zusammenstellten, die Gegenstände beinhalteten, welche die Streitkräfte der Al-Qaida im Irak gegen die Truppen der Amerikaner und ihre Verbündeten unterstützen. Diese Listen umfassten Gegenstände wie GPS (Global Positioning System) Geräte, Nachtsichtgeräte, Schlafsäcke, Prepaid-Telefone, Überlebensmesser und Zelte.
[53]

Laut [55] bekommen virtuelle Währungen immer mehr Bedeutung, da sie eine Möglichkeit der Finanzierung bieten, welche es erlaubt anonym zu bleiben. Die terroristische Organisation Islamischer Staat finanziert sich laut [56] über den illegalen Verkauf von Antiquitäten im Dark Web. Die Autorin aus [56] sieht das Problem darin, dass die Akteure sich aufgrund der Anonymität, die im Dark Web herrscht, regelrecht angezogen fühlen. Des Weiteren liefert sie im Zuge ihrer Arbeit Ansätze dazu, wie man diese Anonymität aufheben kann und die Akteure identifizieren kann.

2.4. Psychologische Aspekte von Cyber-Terrorismus

Eines der Ziele von Terrorismus kann es sein die Bevölkerung eines Landes einzuschüchtern (siehe Kapitel 1.1. Begriffserklärungen). Demnach kann es eine wichtige Rolle spielen psychologisch Einfluss auf die Bevölkerung zu nehmen, um die begangenen Taten möglichst einschüchternd zu gestalten, damit die Wirkung umso stärker wird. Dies kann wiederum die Wahrscheinlichkeit erhöhen, dass die eigentlichen Ziele, tatsächlich erreicht werden. Diese Ziele können beispielsweise Veränderungen im Sinne der Terroristen sein, die die eingeschüchterte Regierung oder die Bevölkerung eines Landes aus Angst vor Angriffen durchführt.

Die Autoren aus [57] beschreiben die systematische Verbreitung von Bildern, die Terroranschläge möglichst dramatisch zeigen, um die Bevölkerung eines Landes (im Fall von [57] ist das Deutschland) einzuschüchtern.

[5] Das arabische Wort „irhabi" (in arabischer Sprache orignal „إرهابي" geschrieben) bedeutet zu Deutsch übersetzt „Terrorist".
[6] Al-Qaida ist ebenfalls arabisch und bedeutet zu Deutsch übersetzt „Die Basis"

Die Schuld für die Verbreitung der Bilder wird allerdings nicht nur den Terroristinnen und Terroristen, sondern auch den Medien zugeschrieben [25], da diese die Bilder ebenso verbreiten, um ihre Reichweite und damit die Verkaufszahlen zu steigern.

Eine weitere bereits kurz erwähnte Arbeit von [38] beschäftigt sich noch genauer mit den psychologischen Effekten von Cyber-Terrorismus. In ihrer Arbeit [38] bringen die Autoren folgende Schlussfolgerung, welche in den Arbeiten von [58] und [59] bereits gezogen wurde, nämlich, dass es nicht auf die Anzahl der Opfer ankommt, die bei einem Anschlag getötet werden, sondern auf die Zahl der Zuschauer, die dadurch beeinflusst werden. Die beispielhafte Statistik aus [60] (Die 15 größten Terrorgruppierungen nach [60] finden sich in Tabelle 6: Terrorakte nach Gruppierungen 2013 bis 2017 [60]. Bei den Anschlägen handelt es sich um alle Arten von Anschlägen, die nicht unbedingt im Zusammenhang mit Cyber-Terrorismus stehen müssen.) zeigt bei den 15 größten Terrorgruppen, dass zwar auf den ersten Blick sehr viele Menschen bei Terroranschlägen im Zeitraum zwischen 2013 bis 2017 getötet wurden, aber verglichen damit wie viele Personen gesamtheitlich die Welt bevölkern ist das immer noch sehr wenig bei einem Vergleich von etwa 78.000 zu etwa 7,7 Milliarden [61]. Nimmt man die Verletzten dazu verdoppelt sich die Anzahl in etwa, aber bleibt trotzdem noch immer vergleichsweise gering. Auch in beiden Weltkriegen starben weit mehr Personen, als bei den Anschlägen im Zeitraum 2013 bis 2017 (Etwa 9,4 Millionen Soldatinnen und Soldaten im ersten Weltkrieg [62] und etwa insgesamt 65 Millionen Tote im 2. Weltkrieg [63] zit. n.).

Nimmt man die Statistik aus [60] und berechnet wie viele Tote tatsächlich durchschnittlich pro Anschlag gestorben sind so sind dies bei den größten 15 Vereinigungen nach [60] meist nur 2 bis 3 Personen. Basierend auf diesen Fakten ist es kein Ziel von Terroristinnen und Terroristen mit Anschlägen für viele Tote in der breiten Masse der Bevölkerung zu sorgen. Zusätzlich kann es aber auch sein, dass sich Terrorgruppen zu schwach für einen Krieg fühlen und deshalb aus taktischen Gründen „nur“ Anschläge durchführen, um den Gegner zu schwächen [25] [64]. Osama bin Laden, der ehemalige Anführer der Al-Qaida, sagte angeblich [25] zu seinen Anhängerinnen und Anhängern sie sollen die Wirtschaft der Amerikaner schwächen, da sie daraus ihre Stärke beziehen.

Gruppierung	Region	Anschläge	Getötet	Verletzt	Geiseln	Getötet pro Anschlag
Taliban	Afghanistan, Pakistan	4.675	19.537	20.796	4.559	4,18
Islamischer Staat	weltweit	5.665	32.280	33.312	21.963	5,70
Boko Haram	West-Afrika, Zentral-Afrika	1.634	16.108	7.575	2.828	9,86
Al-Shabaab	Ost-Afrika	1.619	4.594	4.172	2.011	2,84
Maoisten	Indien, Nepal	1.102	541	518	904	0,49
New People's Army	Philippinen	822	436	440	621	0,53
Kurdische Arbeiter Partei	Asien, Europa	599	530	1627	253	0,88
Al-Qaida	weltweit	550	1.627	2319	320	2,96
Communist Party of India - Maoist	Indien	393	400	291	369	1,02
Houthi extremists	Jemen, Saudi-Arabien	372	532	788	246	1,43
Revolutionary Armed Forces of Colombia	Kolumbien, Panama	288	125	422	51	0,43
Donetsk People's Republic	Ukraine	259	821	584	166	3,17
Abu Sayyaf	Philippinen, Malaysia	240	111	253	303	0,46
Fulani extremists	West-Afrika, Zentral-Afrika	223	1135	184	65	5,09
National Liberation Army of Colombia	Kolumbien	208	119	188	131	0,57
Gesamt	-	18.649	78.896	73.469	34.790	2,64

Tabelle 6: Terrorakte nach Gruppierungen 2013 bis 2017 [60]

Die Autoren aus [38] sehen das ähnlich, erwähnen, dass die Anzahl der Toten gering ist, aber die die noch leben werden von Angst in ihrem täglichen Leben verfolgt. Konventioneller Terrorismus erreicht diese Ziele bereits, [38] stellt sich jedoch die Frage, ob dies mit Cyber-Terrorismus auch funktioniert.

Im Zuge der Arbeiten von [38] wurden zwei Gruppen von Personen mit unterschiedlichen Szenarien von Cyber-Angriffen konfrontiert. Die erste Gruppe wurde zu dem gut dokumentierten Fall aus dem April 2015, dass die Hacktivisten-Gruppe „Anonymus“ Israel aus dem Cyberspace drängen möchte, interviewt. Der zweiten Gruppe wurden Filme, dass die Terrorgruppe Hamas die Trinkwasserversorgung von Israel sabotieren kann, indem zu viel Chlor zugeführt wird, gezeigt. Zusätzlich wurden drei weitere andere Gruppen mit Inhalten konfrontiert. Eine Gruppe mit neutralen Inhalten, eine Gruppe mit nicht tödlichen Cyber-Angriffen und eine Gruppe mit konventionellen Terroristenangriffen. Schließlich wurde die Angst, sowie die Bedrohungswahrnehmung und Unsicherheit der Teilnehmerinnen und Teilnehmer gemessen. Zur Messung der Angst wurde das State-Trait Anxiety Inventory von [65] verwendet. Das Ergebnis ist in Abbildung 5: Angst bezüglich Terrorismus [38] zu sehen. Die Eigenschaften der vier Gruppen getesteten Gruppen nochmal kurz im Überblick:

- Konventioneller Terrorismus: Enthielt Todesfälle und Verletzte
- Tödlicher Cyber-Terrorismus: Enthielt ebenfalls Todesfälle und Verletzte
- Nicht tödlicher Cyber-Terrorismus: Definiert als Offenlegung von Kontoinformationen, Verlust von Geldern
- Kontrollgruppe: Sie wurde keinen terroristischen Inhalten ausgesetzt

[38]

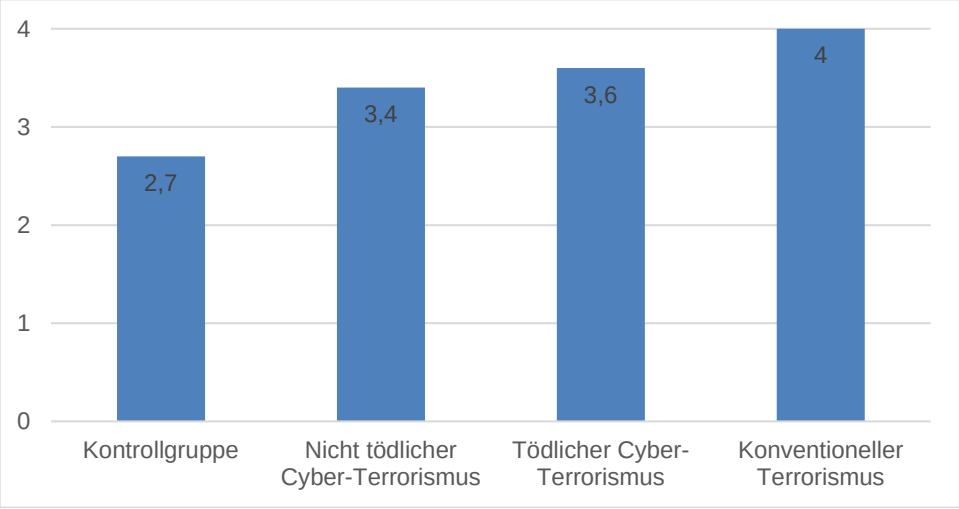


Abbildung 5: Angst bezüglich Terrorismus [38]

Des Weiteren wurden die gleichen Teilnehmerinnen und Teilnehmer aus [38] von den Autoren dazu befragt, welche Maßnahmen Regierungen auf Basis der ihnen gezeigten Vorfälle treffen sollten. Hinsichtlich dessen wurde darauf geachtet hier die Unterschiede zwischen der Gruppe, der die Angriffe von Anonymus, und der Gruppe, der die potenziellen Angriffe von Hamas gezeigt wurden, herauszuarbeiten. Die Ergebnisse sind in Abbildung 6: Prozentuale Zustimmung zu Überwachung und staatlicher Regulierung [38] zu sehen und enthalten die prozentualen Werte der Zustimmung für eine Überwachung für folgende Fragestelllungen:

- „Should the government monitor emails and social networks for suspicious phrases?“ [38]
- „Are you willing to let the government read emails to improve personal and national security?“ [38]
- „Should the government require businesses to install cyber security systems?“[7] [38]

Interessant ist in Abbildung 6: Prozentuale Zustimmung zu Überwachung und staatlicher Regulierung [38] vor allem, dass die Gruppe der potenziellen Hamas Angriffe mehr Bereitschaft für Überwachung zeigt, als die Anonymus Gruppe. Eine letzte Umfrage der Teilnehmerinnen und Teilnehmer befasste sich mit der Fragestellung, ob die Regierung zu Vergeltungsschlägen gegen die Angreifer ausholen soll. Dabei wurde wieder in die Anonymus- und die Hamas-Gruppe unterschieden. Die Autoren gaben 4 Möglichkeiten, die die Regierung zur Vergeltung machen sollte, vor:

- Kleine Cyber-Vergeltung: Cyber-Angriff auf militärische Ziele
- Große Cyber-Vergeltung: Cyber-Angriff auf militärische und zivile Ziele
- Kleine konventionelle Vergeltung: Raketen, Bomben und Artillerie auf militärische Ziele
- Große konventionelle Vergeltung: Raketen, Bomben und Artillerie auf militärische und zivile Ziele

Die Ergebnisse dieser Befragung sind in Abbildung 7: Prozentuale Bevorzugung der Vergeltungsmaßnahmen [38] ersichtlich. Generell kommen die Autoren aus [38] zu dem Schluss, dass die befragten Personen nach den Cyber-Angriffen nicht nur unter Angst leiden, sondern auch das Bedürfnis nach Schutz haben, weshalb sie auch nicht vor Überwachung und Vergeltungsschlägen zurückschrecken.

[7] Zu Deutsch:
- Sollte die Regierung E-Mails und soziale Netzwerke auf verdächtige Formulierungen überwachen?
- Sind Sie bereit, die Regierung E-Mails lesen zu lassen, um die persönliche und nationale Sicherheit zu verbessern?
- Sollte die Regierung von den Unternehmen verlangen, Cyber-Sicherheitssysteme zu installieren?

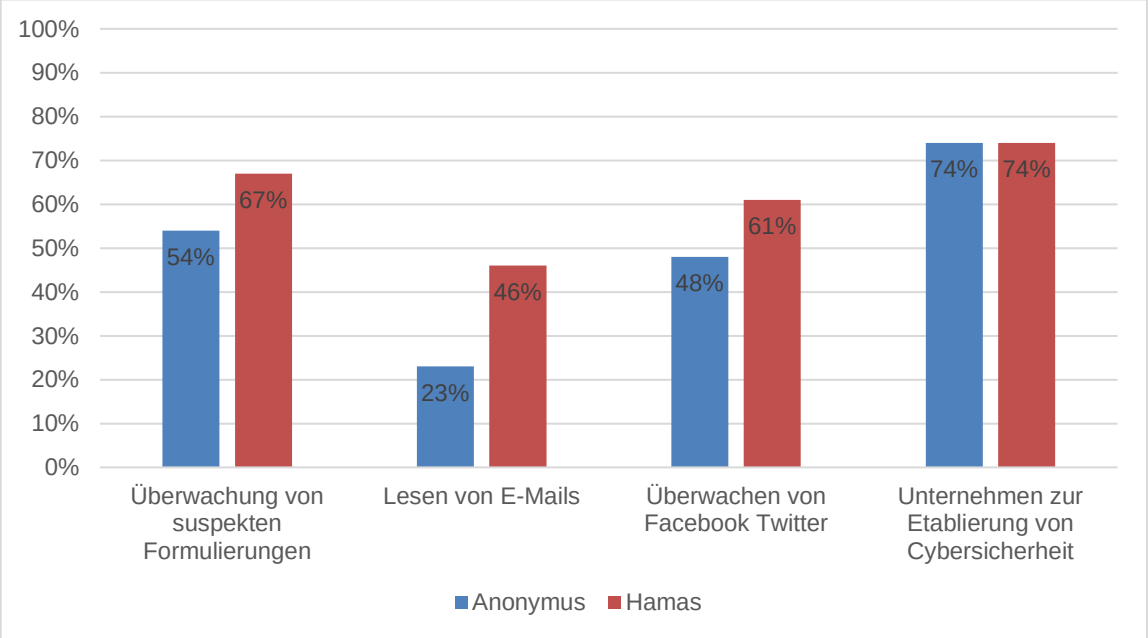


Abbildung 6: Prozentuale Zustimmung zu Überwachung und staatlicher Regulierung [38]

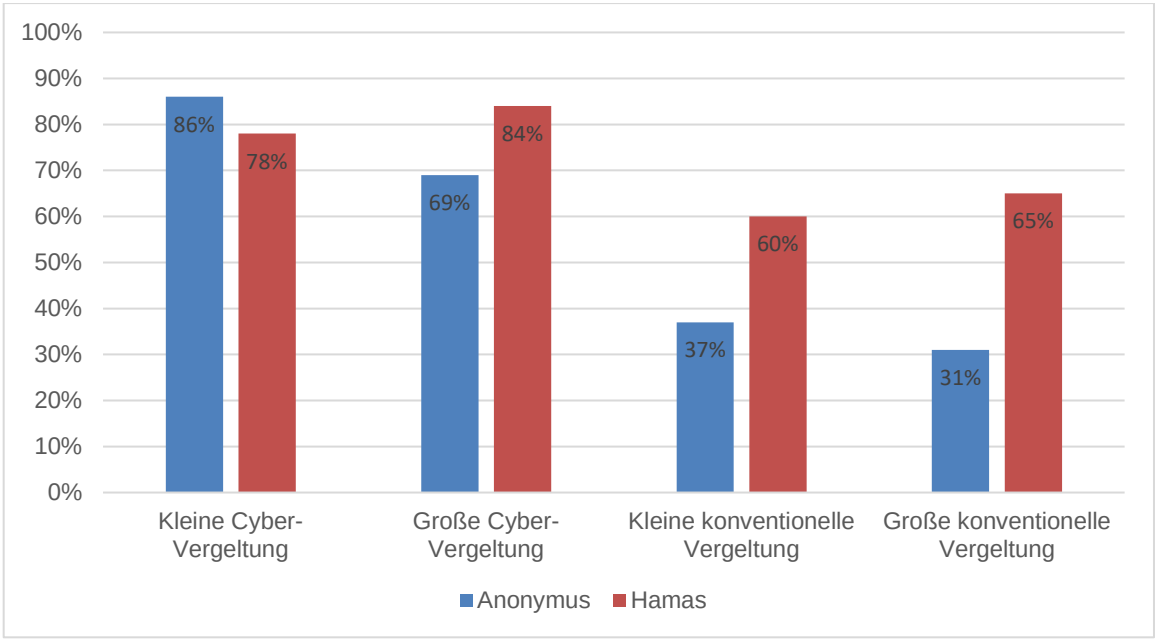


Abbildung 7: Prozentuale Bevorzugung der Vergeltungsmaßnahmen [38]

2.5. Ziele von Terroristinnen/Terroristen

Für das Begehen einer terroristischen Straftat benötigt es ein Ziel (siehe Kapitel 1.1. Begriffserklärungen). Der Täter oder die Täterin, beziehungsweise die Täterinnen oder die Täter müssen also ein geeignetes Ziel aussuchen, das beim Erreichen den gewünschten Effekt bringt. Nicht nur die Terroristinnen und Terroristen selbst müssen nach geeigneten Zielen suchen, sondern auch jene Personen, die für das potenzielle Ziel verantwortlich sind und/oder selbst das Ziel sein könnten profitieren davon den Terroristinnen und Terroristen einen Schritt voraus zu sein. Die zwei größten Vorteile, die sich für Terroristinnen und Terroristen im Cyberspace ergeben sind laut [66] „surprise and anonymity“[8] [66]. Die Autoren aus [66] sind der Meinung, dass es fast unmöglich ist Cyber-Terrorismus auf taktischer Ebene hinsichtlich Ort, Zeitpunkt und Art und Weise des Angriffs vorherzusagen. Jedoch ist man in [66] der Ansicht, dass man auf operativer Ebene, also der Art und Weise wie Cyber-Terroristinnen und Cyber-Terroristen planen Informationstechnologie und automatisierte Tools einzusetzen, sehr wohl präventiv Maßnahmen ergreifen kann, um den Terroristinnen und Terroristen zumindest keinen Schritt im Nachteil zu sein. Zusätzlich ist man in [66] der Ansicht, dass auch potenzielle Ziele von Terroristinnen und Terroristen vorab identifiziert und zu einem gewissen Grad Angriffe vorhergesagt werden können. Um diesen Problemen zu begegnen wird in der Arbeit von [66] jeweils ein Vorschlag gemacht, wie man der „Überraschung“ und der „Anonymität“ entgegenwirken kann.

Damit Terroristinnen und Terroristen das Überraschungsmoment nicht mehr so stark auf ihrer Seite haben schlagen die Autoren [66] das Einrichten eines „Cyber Intelligence Analysis Center“ vor. Dieses soll in der Lage sein, Angriffe vorherzusagen, zu vermeiden oder die Angreiferinnen und Angreifer abzuschrecken, damit sie den Angriff doch nicht durchführen. Dies soll laut [66] grundsätzlich so funktionieren, dass sehr viele Daten über die Aktivitäten von Terroristinnen und Terroristen im Internet gesammelt werden. Mittlerweile wurden Projekte gestartet, die online nach terroristischen Aktivitäten suchen und mit der Idee aus [66] vergleichbar sind. Eines davon ist beispielsweise „REDALERT“ [67]. Das Problem der Anonymität würde sich laut [66] dadurch beheben lassen, dass das Internet grundsätzlich verändert wird und jeder der einen Zugriff haben möchte sich eindeutig identifiziert. Die Lösung bezüglich Anonymität, die [66] präsentiert, wurde allerdings nach mehr als 15 Jahren der Erstveröffentlichung noch nicht umgesetzt. Bei manchen Cyber-Angriffen bis heute nicht geklärt, wer hinter ihnen steht [25].

Einige Ansätze darüber, weshalb Terroristinnen und Terroristen ein bestimmtes Ziel ausgesucht haben finden sich in [68]. Genauer gesagt untersuchen die Autoren, welche Ziele in Europa für Anschläge von Dschihadisten ausgewählt wurden. Dabei werden bestehende Analysen herbeigezogen und untersucht, ob diese genutzt werden können, um besser einschätzen zu können, was die Ziele von Terroristinnen und Terroristen in Europa sein könnten. [69] beschreibt, dass das Ziel von Cyber-Terroristinnen und Cyber-Terroristen nicht das einzelne Individuum, sondern vielmehr das Beeinträchtigen des Wohlbefindens der Gesellschaft als Ganzes ist. Der Autor aus [25] ist der Ansicht, dass Terroristinnen und Terroristen zivile Ziele Militärischen gegenüber bevorzugen, weil sie viel verwundbarer sind und nach Meinung von [25] vermutlich mehr Aufmerksamkeit in den Medien verursachen.

In [70] untersucht der Autor einige Fälle von weltweiten Cyber-Angriffen seit 1998. Die Fälle werden untereinander verglichen, wodurch ein Scoring System entsteht. Dieses beschreibt, wie wahrscheinlich gewisse Arten von Cyberangriffen sind und wie groß die Auswirkungen sein können.

Eine andere Herangehensweise an die Erkennung potenzieller Ziele von Terroristinnen und Terroristen ist, nicht nach den Angriffszielen zu suchen, sondern auszuschließen, welche Regierungen, Unternehmen, Personen oder ähnliches mit großer Wahrscheinlichkeit nicht angegriffen werden. So argumentiert beispielsweise [71], dass online genutzte Unterstützungstools, die von Terroristinnen und Terroristen zur Koordination genutzt werden, ein unwahrscheinliches Angriffsziel sind, da ein Angriff auf Systeme und Tools, aus denen man einen Vorteil zieht, äußerst unvorteilhaft und kontraproduktiv ist.

[8] Zu Deutsch: Überraschung und Anonymität

2.6. Angriffsmethoden der Cyber-Terroristin/des Cyber-Terroristen

Wenn die Cyber-Terroristin oder der Cyber-Terrorist ein Ziel gefunden hat, gibt es verschiedene Möglichkeiten, wie sie oder er dieses Ziel angreifen, manipulieren, beeinflussen oder zerstören kann. Laut [20] und [26] zielen die meisten Angriffe darauf ab, das Zielsystem zu stören, Daten zu löschen oder einen Systemausfall zu provozieren. Zusätzlich wird noch erläutert, dass es aber auch Angriffe gab, die das angegriffene System selbst zerstört haben. Das bekannteste Beispiel dafür ist Stuxnet [72]. Was man mit Cyberangriffen alles bewirken kann wird zum Beispiel in [73] beschrieben.
Eine gute Auflistung über die aktiven und passiven „Waffen", also Möglichkeiten einen Angriff aktiv durchzuführen beziehungsweise passive Methoden, die zusätzlich, aber nicht direkt zum Erfolg eines Angriffs beitragen, findet sich beispielsweise in der Arbeit von [74]. Folgende Tools und Methoden werden erwähnt und zusätzlich erläutert:

- Hacken: Dies ist die populärste Methode, die von Terroristinnen und Terroristen genutzt wird. In diese Kategorie gehören Aktivitäten wie Paket sniffing, Tempest Angriffe[9], das Hacken von Sicherheitsfirewalls, das Knacken verschlüsselter Passwörter und das Verursachen von Buffer Overflows.
- Trojaner: Programme, die vorgeben etwas anderes zu tun, als sie eigentlich wirklich tun.
- Computerviren: Ein Programm, das in andere Programme einschleust wird und Störungen verursacht.
- Computerwürmer: Eigenständige Programme, die Kopien von sich über Netzwerkverbindungen an andere Computer übertragen.
- E-Mail Hacking und Online-Identitätsdiebstahl: Computerviren und -würmer verbreiten sich in bestehenden Programmen und versuchen über eine Internetverbindung andere Systeme zu erreichen. Die Verbreitung erfolgt beispielsweise als E-Mails oder es werden mit der übernommenen E-Mail-Identität Inhalte unter der Identität des Opfers versandt.
- Denial of Service Angriffe: Dadurch wird der Person, die ein Computersystem verwenden möchte, die Möglichkeit genommen das System zu nutzen.
- Kryptografie: Terrorgruppen verwenden Verschlüsselung, um Sprach- und Datenübertragungen davor abzusichern abgehört zu werden.

[74]

In Bezug auf Kapitel 2.5. Ziele von Terroristen bedeutet das, dass je nachdem was die Terroristinnen und Terroristen mit dem Angriff bewirken wollen oder anders ausgedrückt, abhängig davon worin der größte Vorteil liegt, unterschiedliche Angriffsmethoden genutzt werden. Im Beispiel von Younis Tsouli [52] [53] aus Kapitel 2.3. Finanzierung von Terrorismus, welcher Kreditkarten mithilfe von Phishing und Trojanern gestohlen hat bedeutet das, dass es in seinem Fall keinen Sinn macht die Organisationen, welche die Kreditkarten ausgestellt haben, beispielsweise mit Denial of Service Angriffen oder Computerviren anzugreifen, da er sich so selbst schaden würde und unter Umständen die gestohlenen Kreditkarten nicht verwenden könnte. Außerdem würden zusätzliche Angriffe sowohl auf die Kartenaussteller und die betroffenen Privatpersonen nur deren Misstrauen erhöhen und somit möglicherweise eine schnellere Sperre der gestohlenen Karten bewirken.

[9] Dabei handelt es sich um Angriffe, die darauf abzielen aufgrund der elektrischen Strahlung/Ausstrahlung eines Computers zu sensiblen Informationen, wie Schlüsseln zu gelangen [174]

2.7. Kriminologische Ansätze

Diese Arbeit bewegt sich im Umfeld der Kriminologie, also den Ursachen und Erscheinungsformen von Verbrechen und deren Bekämpfung [75], im Bereich Vermeidung von Cyber-Terrorismus. Informationssicherheitsmanagement besteht aus einigen Aspekten, die von einem Unternehmen, das entsprechende IT-Systeme einsetzt, beachtet werden müssen, damit dieses funktioniert:

- Deterrence: Abschrecken des Angreifers, sodass es nicht zu einem Angriff kommt
- Prevention: Abwehren des Angriffs durch entsprechende Sicherheitsmechanismen
- Detection: Erkennen eines Angriffs, zum Beispiel im Monitoring
- Recovery: Wiederherstellung der Systeme

[76] [77]

Diese Aspekte sind auch als eine Art Abstufung zu betrachten. Das heißt zunächst kann man versuchen die Angreiferin oder den Angreifer abzuschrecken. Wenn das nicht funktioniert kann der Angriff durch entsprechende Maßnahmen abgewehrt werden. Sollte das auch nicht funktionieren ist es möglich durch ein Monitoring System den Angriff zu erkennen und sofort zu handeln. Schließlich bleibt bei einem unentdeckten Angriff nur noch die Möglichkeit wenigstens nachträglich vorbereitet zu sein, um alles schnellstmöglich wiederherzustellen. Der Fokus dieser Arbeit liegt hauptsächlich auf den ersten Punkten Deterrence und Prevention. Auf dem Gebiet der Kriminologie gibt es bereits Ansätze, die sich mit dem Thema Vermeidung von Kriminalität beschäftigen. Dies gilt sowohl allgemein für Kriminologie in der realen Welt und auch in der Cyber-Welt verbunden mit Cyber-Terrorismus.

Einen guten Überblick über die Vermeidung von Verbrechen in der realen Welt zeigen die Autoren aus [78]. Ferner bieten sie einen umfangreichen Literaturüberblick bezüglich der Vermeidung von Kriminalität in den letzten Jahren. Im Zuge dessen wird untersucht wie sich Polizeiaufkommen, drohende Strafen und lokale Arbeitsmarktbedingungen auf die Kriminalität auswirken. Die Autoren kommen zu dem Schluss, dass sich eine größere Anzahl an Polizistinnen und Polizisten, die effektiv eingesetzt wird, positiv auf die Vermeidung von Verbrechen auswirkt. Was die Strafvollziehung angeht kommt man zu dem Ergebnis, dass drohende Strafen prinzipiell schon abschreckend sind, aber umso effektiver sind, desto härter sie bei manchen speziellen Fällen werden können. In anderen Worten soll das heißen, man sollte Terrorismus nicht einfach hart bestrafen, sondern spezieller differenzieren, wie sich das Strafausmaß beispielsweise bei Drohungen, Sachbeschädigungen, schweren Verletzungen oder Mord ändert. Wesentlich ist hierbei, bei schwereren Delikten das Strafmaß deutlich zu erhöhen. Was die Arbeitsbedingungen betrifft kommt man zu dem Schluss, dass es auch hier Zusammenhänge zwischen fehlenden Arbeitsplätzen und/oder schlechten Arbeitsbedingungen gibt. Basierend auf den Ergebnissen dieser Arbeit stellen sich zwei Fragen:

- Gelten diese drei Faktoren (Polizeiaufkommen, Strafmaß, Arbeitsbedingungen) für herkömmlichen Terrorismus genauso wie für Kriminalität?
- Sind diese drei Faktoren für Cyber-Terrorismus ebenfalls anwendbar? Wenn nicht, was ist der entsprechende komplementäre Aspekt im Cyberspace?

[78]

In Bezug auf die laut österreichischem Gesetz terroristischen Straftaten [14] sind die dort angeführten Straftaten auch ohne terroristischen Hintergrund strafbar. Dann sind es keine Terrorhandlungen, sondern „normale“ Straftaten. Dies ergibt sich durch die abschließende Bedingung, die unter § 278c Absatz 1 BG [14] angeführt ist („wenn die Tat geeignet ist […] ernsthaft zu erschüttern oder zu zerstören.“ [14], siehe Kapitel 1.1. Begriffserklärungen). Da sich die Ergebnisse von [78] auf Straftaten beziehen und auch [14] Straftaten beinhaltet sind Polizeiaufkommen, drohende Strafen und Arbeitsmarktverhältnisse in den meisten Fällen auch auf terroristische Straftaten anwendbar. Lediglich das Polizeiaufkommen ist bezüglich § 278c Absatz 1 BG Punkt 6 [14] bei Cyber-Terrorismus nicht immer zielführend. Die Angriffe können von den Täterinnen und Tätern abgelegen von jeglicher Polizeipräsenz stattfinden und zahlreiches Schutzpersonal an den betroffenen Zielen kann die Angreiferin oder den Angreifer nicht abschrecken den Angriff durchzuführen, da diese beziehungsweise dieser sein Ziel physisch nicht unbedingt aufsuchen muss und daher gar nicht sieht, wer sie beziehungsweise ihn aufhalten möchte.

Im Cyberspace muss das Personal, welches zum digitalen Schutz eines Computersystems eingesetzt wird, entsprechend aus IT-Sicherheitsexpertinnen beziehungsweise IT-Sicherheitsexperten oder Ähnlichem bestehen. Denn es gilt, wie in der analogen Welt, dass diese Expertinnen und Experten die Angreiferin oder den Angreifer erwischen können. Dafür müssen diese Expertinnen und Experten Sputen von Angreiferinnen und Angreifern zurückverfolgen können, ähnlich wie die Polizei versucht eine Straftäterin oder einen Straftäter zu fassen indem sie sie oder ihn verfolgt. Die Angreiferin oder der Angreifer muss daher darauf aufmerksam werden, dass sie beziehungsweise er von professionellen IT-Sicherheitsexpertinnen oder IT-Sicherheitsexperten erwischt werden kann und dann festgenommen werden kann. Die Präsenz von entsprechenden Systemen und dem dazugehörigen Personal könnte daher schon eine abschreckende Wirkung haben und dafür sorgen, dass Die Angreiferin oder der Angreifer verunsichert wird. Es muss der Eindruck vermittelt werden, dass ein Angriff Konsequenzen haben kann, wenn die Täterin oder der Täter zu unvorsichtig ist und sich zu viele Fehler leistet.

Weitere mögliche Maßnahmen, die dazu führen, dass ein Cyber-Angriff nicht stattfindet beschreibt [77]. Ferner werden zwei Modelle aufgegriffen, nämlich die „Rational Choice Perspective“ und die „Situational Crime Prevention“. Die Rational Choice Perspective geht davon aus, dass Verbrechen allgemein deshalb passiert, weil die Täterinnen und Täter einen Vorteil oder Nutzen daraus ziehen [77]. Für Verbrechen ist das beispielsweise Geld oder materielles Gut, für Terrorismus gelten die bereits genannten Ziele unter [14], also beispielsweise das Stürzen eines Staatsoberhauptes, das Bedrohen und Einschüchtern der Bevölkerung oder das Hacken von Anlagen, die zur Trinkwasserversorgung dienen. Des Weiteren kann Verbrechen unter unterschiedlichen Rahmenbedingungen geschehen [77]. [77] vergleicht das mit einem Autodiebstahl, weil jemand das Auto weiterverkaufen möchte und mit einem Autodiebstahl, weil jemand nur temporär von einem Ort zum anderen möchte. Ein Beispiel für dieses Joyriding bei klassischen (ohne Cyber-Angriff) Terroristinnen und Terroristen ist, dass sie bei ihrer Flucht ebenfalls ein Auto entwenden können. Da es bereits Fahrzeuge mit umfassender technischer Ausstattung gibt, können diese aber von Cyber-Terroristinnen und Cyber-Terroristen gehackt werden und für missbräuchliche Zwecke genutzt werden, die bis zu Mord reichen [79] [80]. Außerdem unterscheidet die Rational Choice Perspective bei kriminellen Entscheidungen zwischen „Involvement“ (Teilnahme) und „Event“ Entscheidungen [77].

Bei Involvement geht es um die allgemeine Teilnahme an den kriminellen Aktionen [77]. Die Täterin oder der Täter muss sich dazu entscheiden, wann sie beziehungsweise er damit beginnt, wie lange sie oder er aktiv bleibt und wann beziehungsweise ob sie oder er wieder aussteigt. [77] Evententscheidungen beziehen sich auf die Durchführeng einer Straftat [77], also beispielsweise alle Schritte, die sich die Täterin oder der Täter vorher überlegt, wenn sie oder er eine Bank überfällt. Für einen Banküberfall überlegt man beispielsweise folgende Aktionen: Wie läuft der Transport der Beute?, die Ankunft bei der Bank?, das Betreten des Gebäudes?, Wie lange bleibt man dort?, Wo bringt man die Beute unter?. Analoge Fragestellungen für die Cyber-Terroristin oder den Cyber-Terroristen könnten beispielsweise Welche Angriffsmethode setze ich ein? Wie heble ich Sicherheitsmechanismen aus? Wie verwische ich meine Spuren? Wo liegen Schwachstellen in der Infrastruktur? sein. Situational Crime Prevention beschäftigt sich damit, dass nicht die Ursachen von kriminellem Handeln beseitigt werden, sondern bestimmte Techniken zum Einsatz kommen, die das Verbrechen an sich weniger lukrativ erscheinen lassen [77]. Es gibt bereits einige Techniken zur Prävention von Verbrechen [81], welche in Tabelle 7: 25 Techniken für Situational Crime Prevention [81] ersichtlich sind. Diese 25 Techniken werden in 5 Kategorien eingeteilt, welche die erste Zeile von Tabelle 7 bilden [81].

[77] versucht nun die Modelle Rational Choice Perspective und Situational Crime Prevention auf Informationssicherheit anzuwenden. Beginnend mit der Rational Choice Perspective werden von [77] zwei Fälle von Kriminalität in ihrem Ablauf und Aktionen gegenübergestellt und miteinander verglichen. Der erste Fall stammt aus der analogen Welt von [82] und behandelt einen U-Bahn Überfall. Der zweite bezogen auf Informationssicherheit stammt aus [83] und handelt von einem Mitarbeiter aus einem Gemeinderat, welcher aufgrund der schlechten Sicherheitsvorkehrungen (Kollegen sperrten ihre Bildschirme nicht) die Computer seiner Kolleginnen und Kollegen dazu benutzen konnte falsche Rechnungen auszustellen. Beide Fälle sind in ihren Abläufen und Tätigkeiten in Tabelle 8: Vergleich der Fälle aus [81] und [83] nach [77] ersichtlich. Hierbei wurde sehr genau auf die einzelnen Schritte eingegangen, die zu bedenken sind, wenn man die beiden Verbrechen begehen möchte. Nachdem nun der Ablauf in Tabelle 8 Spalte 3 festgelegt wurde fährt [77] damit fort entsprechende Techniken für Situational Crime Prevention nach [81] abzuleiten.

Das Ergebnis von [77] enthält den Ablauf und die Tätigkeiten in den ersten beiden Spalten, sowie entsprechende Vermeidungsmaßnahmen in den restlichen Spalten, welche der aktuellen Phase, in der Aktionen von der Täterin

beziehungsweise vom Täter gefordert sind, zugeordnet sind (siehe Tabelle 9: Gegenmaßnahmen bei computerbezogener Kriminalität [77]). In Tabelle 9 ist zusätzlich zu beachten, dass die Spalten „Reduce the rewards“, „Reduce provocation“ und „Remove excuses“ nicht wie im Original aus [77] vorhanden sind, da sie keinen Inhalt bieten. Dies bedeutet aber nicht, dass bei Computer-Kriminalität immer davon auszugehen ist, dass man keine wirksamen Maßnahmen in diesen Bereichen durchführen kann. Der betrachtete Fall von [77] handelte von einem Mitarbeiter des Gemeinderats und die abgeleiteten Gegenmaßnahmen arbeiten hauptsächlich auf nicht-technischer Ebene. Ob und wie sich diese Maßnahmen für Cyber-Terrorismus anwenden lassen soll abschließend (Kapitel 5) mithilfe der neun betrachteten Fälle von Cyber-Terrorismus ergründet werden.

Die Autoren aus [64] haben sich speziell mit dem Thema Vermeidung von Cyber-Terrorismus beschäftigt. Sie vertreten die Ansicht, dass die Erhöhung der drohenden Strafen allein nicht zielführend ist, da vor allem im Vordergrund stehen muss die Täterinnen und Täter überhaupt zu erwischen. Nur so können die Terroristinnen und Terroristen zu ihrer Strafe kommen. Die zu beachtenden abschreckenden Aspekte, die Cyber-Terrorismus verhindern, teilen sie in folgende drei Gruppen ein:

- „technical“ [64]: Die technischen Mittel umfassen alle Möglichkeiten, die dazu beitragen Terroristinnen und Terroristen zu identifizieren.
- „policy“ [64]: Festgelegte Standards in Richtlinien dazu, wie oft ein Unternehmen oder eine Regierung Informationen über Data Breaches veröffentlicht.
- „legal“ [64]: Rechtliche Grundlagen auf Basis derer Cyber-Terroristen verfolgt werden dürfen.

In jedem Fall ist man der Ansicht, dass Cyber-Terroristinnen und Cyber-Terroristen der Eindruck vermittelt werden muss, dass man sie erwischen und identifizieren kann. Das Problem dabei ist, die Terroristinnen und Terroristen darauf aufmerksam zu machen. Dafür wird vorgeschlagen über festgenommene Cyber-Terroristinnen und Cyber-Terroristen im Fernsehen und Zeitungen zu berichten.
[64]

Increase the effort	Increase the risks	Reduce the rewards	Reduce provocation	Remove excuses
1. Target harden: ■ Steering column locks and immobilisers ■ Anti-robbery screens ■ Tamper-proof packaging	*6. Extend guardianship:* ■ Take routine precautions: go out in group at night, leave signs of occupancy, carry phone ■ "Cocoon" neighborhood watch	*11. Conceal targets:* ■ Off-street parking ■ Gender-neutral phone directories ■ Unmarked bullion trucks	*16. Reduce frustrations and stress:* ■ Efficient queues and polite service ■ Expanded seating ■ Soothing music / muted lights	*21. Set rules:* ■ Rental agreements ■ Harassment codes ■ Hotel registration
2. Control access to facilities: ■ Entry phones ■ Electronic card access ■ Baggage screening	*7. Assist natural surveillance:* ■ Improved street lighting ■ Defensible space design ■ Support whistleblowers	*12. Remove targets:* ■ Removable car radio ■ Women's refuges ■ Pre-paid cards for pay phone	*17. Avoid disputes:* ■ Separate enclosures for rival soccer fans ■ Reduce crowding in pubs ■ Fixed cab fares	*22. Post instructions:* ■ "No Parking" ■ "Private Property" ■ "Extinguish camp fires" [sic]
3. Screen exits: ■ Ticket needed for exit ■ Export documents ■ Electronic merchandise tags	*8. Reduce anonymity:* ■ Taxi driver IDs ■ "How's my driving?" decals ■ School uniforms	*13. Identify property:* ■ Property making ■ Vehicle licensing and parts marking ■ Cattle branding	*18. Reduce emotional arousal:* ■ Controls on violent pornography ■ Enforce good behavior on soccer field ■ Prohibit racial slurs	*23. Alert conscience:* ■ Roadside speed display boards ■ Signatures for customs declarations ■ "Shoplifting is stealing"
4. Deflect offenders: ■ Street closures ■ Separate bathrooms for women ■ Disperse pubs	*9. Utilize place managers:* ■ CCTV for double-deck buses ■ Two clerks for convenience stores ■ Reward vigilance	*14. Disrupt markets:* ■ Monitor pawn shops ■ Controls on classified ads ■ License street vendors	*19. Neutralize peer pressure:* ■ "Idiots drink and drive" ■ "It's ok to say No" ■ Disperse troublemakers at school	*24. Assist compliance:* ■ Easy library checkout ■ Public lavatories ■ Litter bins
5. Control tools/weapons: ■ "Smart" guns ■ Disabling stolen cell phones ■ Restrict spray paint sales to juveniles	*10. Strengthen formal surveillance:* ■ Red light cameras ■ Burglar alarms ■ Security guards	*15. Deny benefits:* ■ Ink merchandise tags ■ Graffiti cleaning ■ Speed humps	*20. Discourage imitation:* ■ Rapid repair of vandalism ■ V-chips in TVs ■ Censor details of modus operandi	*25. Control drugs and alcohol:* ■ Breathalyzers in pubs ■ Server intervention ■ Alcohol-free events

Tabelle 7: 25 Techniken für Situational Crime Prevention [81]

Scene/Function	Script Action	Script Action
Preparation	Meet and agree on hunting ground	Deliberately gaining access to the organization
Entry	Entry into underground system	Already authorised as employee
Pre-condition	Travel to hunting ground	Wait for employees absence from offices
Pre-condition	Waiting/circulating at hunting ground	-
Instrumental Pre-Condition	Selecting victim and circumstance	Access colleagues' computers
Instrumental Initiation	Closing-in/preparation	Access programmes
Instrumental Actualisation	Striking at victim	False customer account construction
Instrumental Actualisation	Pressing home attack	-
Doing	Take money, jewelry, etc.	Authorisation of fictitious invoices
Post-Condition	Escape from scene	Exit programmes
Exit	Exit from system	Exit from system

Tabelle 8: Vergleich der Fälle aus [81] und [83] nach [77]

Scene/Function	Script Action	Increase the effort	Increase the risks
Preparation	Deliberately gaining access to the organization	■ Prospective employment screening	
Entry	Already authorised as employee		
Pre-condition	Wait for employees absence from offices	■ Physical segregation of duties ■ Staggered breaks ■ System time outs	■ Signing in/out of offices
Instrumental Pre-Condition	Access colleagues' computers	■ Biometric fingerprint authentication	
Instrumental Initiation	Access programmes	■ Password use for access to specific programmes	
Instrumental Actualisation	False customer account construction		■ Two person sign-off on new accounts
Doing	Authorisation of fictitious invoices		■ Audit of computer logs ■ Budget monitoring
Post-condition	Exit programmes		
Exit	Exit from system		■ User event viewer

Tabelle 9: Gegenmaßnahmen bei computerbezogener Kriminalität [77]

3. Fälle von Cyber Terrorismus

In diesem Kapitel sollen einige ausgewählte Fälle von Cyber-Terrorismus präsentiert werden. Bei der Auswahl der Fälle wurden die in Kapitel „1.2. Cyber-Terrorismus“ festgelegten Rahmenbedingungen, die Cyber-Terrorismus kennzeichnen herangezogen. Dabei ist zu beachten, dass sich hier nicht alle Fälle von Cyber-Terrorismus wiederfinden, unabhängig davon, ob sie mit der hier verwendeten Definition oder einer anderen als potenzielle Fälle von Cyber-Terrorismus betrachtet werden können. Ein kurzer Überblick über alle Fälle, die im Zuge dieser Arbeit behandelt wurden, findet sich in Tabelle 10: Übersicht der behandelten Cyber-Terror-Fälle. Die Spalte Jahr beinhaltet das Jahr, in dem der Fall aufgetreten ist. Damit die Fälle leichter referenziert werden können werden in dieser Arbeit Nummern vergeben und Kurzbezeichnungen verwendet. Eine Übersicht für diese Nummern und Kurzbezeichnungen findet sich ebenfalls in Tabelle 10. Für eine leichtere Zuordnung ist in der Spalte Kurzbeschreibung das wesentlichste des Cyber-Angriffs in wenigen Worten beschrieben.

Jahr	Nummer	Kurzbezeichnung	Kurzbeschreibung
1998	1	Sri Lanka	Die Mailserver von Botschaften Sri Lankas wurden mit zahlreichen Spamnachrichten überflutet. [18] [84] [85]
2000	2	Aum Shinrikyo	Ein japanischer Kult genannt Aum Shinrikyo stiehlt Informationen aus Kernkraftanlagen. [86]
2007	3	Estland	Internetinfrastruktur und -services in Estland wurden von externen Anfragen überflutet und verweigerten ihre Funktion. [87] [88]
2008	4	Georgien	Um die Zeit des russisch-georgischen Krieges fanden Cyber-Angriffe auf Georgien statt [89] [90]
2009	5	Vereinigte Staaten	Das Stromnetz der Vereinigten Staaten wurde Opfer einer Cyber-Spionage-Kampagne. Auch andere Infrastruktur war betroffen [91]
2013	6	Südkorea	Bei einem Cyber-Angriff auf Südkorea wurden drei Fernseh- und Radiosender, sowie drei Banken in ihrem Betrieb gestört. [92] [93]
2014	7	Saudi-Arabien	Die Syrian Electronic Army hackt 17 arabische Webseiten, welche in Verbindung mit der saudi-arabischen Regierung stehen. [94] [95]
2015	8	Ukraine	In drei Regionen der Ukraine wurden lokale Stromversorger gehackt und damit ein Stromausfall verursacht. [96] [97]
2019	9	Israel	Ein Cyber Angriff der Terrorgruppe Hamas wird von den Israel Defense Forces durch einen Luftangriff abgewehrt. [98]

Tabelle 10: Übersicht der behandelten Cyber-Terror-Fälle

Für eine bessere Vergleichbarkeit der untersuchten Fälle werden die Fälle nicht nur beschrieben, sondern es soll im Zuge dessen auf die folgenden Aspekte in jedem cyber-terroristischen Ereignis eingegangen werden (In Klammern befinden sich die verwendeten Überschriften für die Kapitel, welche bei jedem Fall die genannten Aspekte beinhalten):

- Terroristische Gruppe oder Person, die den Angriff durchgeführt hat (Angreiferin/Angreifer)
- Ziel beziehungsweise Opfer des Angriffs (Ziel)
- Beschreibung des Angriffs, sowie Art des Angriffs (Angriff)
- Folgen, die der Angriff hatte beziehungsweise immer noch hat (Folgen)

Die Gruppe oder Person, die hinter dem Angriff steht, ist zunächst deshalb relevant, da somit unterschieden werden kann, ob Cyber-Terrorismus eher von Einzeltätern oder Gruppen durchgeführt wird. Die Informationen

sollen dabei helfen herauszufinden, welche Hintergründe die Täterinnen und Täter haben oder haben könnten, welche Ideologien sie verfolgen und wie sie ihre Ziele ausgewählt haben. Relevant ist hierbei auch welche Kapazitäten die Angreiferinnen und Angreifer hinsichtlich technischer Ausrüstung und Wissen hatten. Unter Umständen kann es sein, dass einem Fall keine Täterin oder kein Täter eindeutig zugewiesen werden kann. Einerseits liegt dies daran, dass die Täterin oder der Täter unerkannt bleiben konnte und ihre beziehungsweise seine Spuren gut genug verwischt hat, andererseits kann es sein, dass sich zwar eine Person oder Gruppe zu dem Fall bekannt hat, dies aber nicht mit überwiegender Sicherheit bestätigt werden kann und Zweifel existieren, die die scheinbare Täterin oder den scheinbaren Täter anzweifeln lassen. Sollte es zu solchen Fällen kommen wird dies unter diesem Punkt (Terroristische Gruppe oder Person, die den Angriff durchgeführt hat) angemerkt.

Informationen über die Firma, Person, Regierung oder ähnliches, die angegriffen wurde sollen dabei helfen besser zu verstehen, welche Ziele ausgewählt werden und um später Ähnlichkeiten herauszuarbeiten. Im Zuge dessen sollen Fragen wie beispielsweise folgende beantwortet werden:

- Welche Sicherheitsmaßnahmen wurden seitens des Opfers getroffen, um Cyberangriffe generell abwehren zu können?
- Welche Informationen konnten die Terroristinnen und Terroristen vorab über ihr Ziel herausfinden?
- Wie wurden die Terroristinnen und Terroristen auf das Ziel aufmerksam? Bestand hier eine Verbindung?

Ein weiterer Aspekt bei den Fällen ist der Angriff selbst, genauer gesagt, wie die Terroristinnen und Terroristen vorgegangen sind, um ihr Ziel zu erreichen. Im Zuge dessen soll analysiert werden, welche Angriffsmethoden in der Vergangenheit eingesetzt wurden und was unter Umständen bekannte Fehler seitens der Ziele waren.

Zuletzt werden in jedem Fall die Folgen des cyber-terroristischen Angriffs erläutert. Dies beinhaltet vorwiegend, aber nicht ausschließlich Schäden aller Art, inklusive Personenschäden physischer und psychischer Art, Umweltschäden, Schäden an der IT-Infrastruktur beim Angriffsziel, sowie weitere Sachschäden. Nachdem ein Ziel hinter terroristischen Anschlägen auch das politische Umdenken sein kann, (vergleiche 1.2. Cyber-Terrorismus) werden auch solche Folgen angeführt.

3.1. E-Mail Spam Sri Lanka Botschaften

Der erste hier präsentierte Fall von Cyber-Terrorismus passierte während des Bürgerkrieges in Sri Lanka. Die E-Mail-Server einiger Botschaften Sri Lankas wurden mithilfe von Denial of Service Angriffen lahmgelegt [18] [84] [85].

Angreiferin/Angreifer
Die größere Gruppierung hinter dem Angriff wird „Liberation Tigers of Tamil Eelam“ genannt und ist sowohl seitens der EU [7] als auch der Vereinigten Staaten von Amerika [8] als terroristische Organisation eingestuft. Die Organisation selbst wurde 1976 gegründet [99] und führte einen Bürgerkrieg gegen die Regierung Sri Lankas. Dieser Bürgerkrieg dauerte von 1983 bis 2009 [100]. In diesen Zeitraum fällt der hier beschriebene cyber-terroristische Angriff aus dem September 1998 [84]. Der Ursprung für den Konflikt und die resultierende Bildung der „Liberation Tigers of Tamil Eelam“ ist, dass sich die Bevölkerung zum größten Teil aus Singhalesen (buddhistische Glaubensrichtung) und Tamilen (hinduistische Glaubensrichtung) zusammensetzt. Während der Kolonialzeit Sri Lankas wurden die sozialen und wirtschaftlichen Rechte der Tamilen stark eingeschränkt. Die Menschen glaubten mit politischen Wegen diese Missstände nicht beseitigen zu können und wendeten Gewalt an [100]. Dadurch ist die Gruppe entstanden und wurde vor allem für ihre Bombenangriffe auf zivile Personen bekannt [99]. Dies führte dazu, dass sie beispielsweise schon seit Oktober 1997 als terroristische Organisation beim Außenministerium der Vereinigten Staaten von Amerika [8] gelistet ist. Den Angriff selbst führte eine Untergruppe der „Liberation Tigers of Tamil Eelam“ durch, nämlich die „Internet Black Tigers“ [85], welche sich im Zuge des Angriffs in einem persönlichen Statement nicht nur zu dem Fall bekannten, sondern auch das vermeintliche Ziel klar machten (siehe Abschnitt Angriff).

Ziel
Das Angriffsziel sind Botschaften Sri Lankas in drei Ländern gewesen (namentlich erwähnt werden in [85] Südkorea, Kanada und die Vereinigten Staaten). Dass der Angriff auf Sri Lanka gerichtet ist, ist in diesem Fall sehr naheliegend, da die „Liberation Tigers of Tamil Eelam“ bereits seit Jahren im Krieg mit der Regierung Sri Lankas stehen [100]. Warum genau Botschaften und deren E-Mail Server ausgewählt wurden, konnte im Zuge der Recherche nicht herausgefunden werden. Naheliegend wäre jedoch damit die Kommunikation Sri Lankas mit der Außenwelt zu stören und den Krieg damit zugunsten der „Liberation Tigers of Tamil Eelam“ zu beeinflussen.

Angriff
Die Angreiferinnen und Angreifer überfluteten die Mail Server von Botschaften Sri Lankas mit etwa 800 Spam Nachrichten pro Tag für über zwei Wochen [18] [85]. Die betroffenen Botschaften befanden sich in Seoul (Südkorea), Ottawa (Kanada) und Washington D.C. (District of Columbia) (Vereinigte Staaten) [85]. Inhalt der Nachrichten war folgende Botschaft: „We are the Internet Black Tigers and we’re doing this to disrupt your communications.“ [18] [85] zit. n. Zusätzlich wurden laut [84] auch Bombendrohungen verschickt. Diese Angriffe resultierten in einen Denial of Service der E-Mail-Server.

Folgen
Diplomatinnen und Diplomaten konnten den E-Mail-Service für ihre täglichen Arbeiten nicht mehr benutzen. Es wurde auch von „E-Mail-Terrorismus“ gesprochen [84]. Physischer Schaden wurde zwar keiner angereichtet, was nicht üblich ist für die Gruppierung, aber dennoch sorgte der Angriff für Angst in den Botschaften [85]. Damit ein solcher Angriff nicht wieder passieren kann wurde laut [84] zit. n. in der Botschaft Washingtons 1999 ein Programm entwickelt, welches die Mails der „Liberation Tigers of Tamil Eelam“ filtert. Obwohl der Angriff erfolgreich verlief und er immerhin die E-Mail-Kommunikation für zwei Wochen lahmlegen konnte, ging der Bürgerkrieg in Sri Lanka nicht zugunsten der Tamil Minderheit aus. Sie wurden im Zuge des Krieges von ihren Kontrahenten, der sri-lankischen Armee, 2009 vernichtend geschlagen [100]. Der Angriff auf die Mailserver wird bis heute teilweise als der erste Cyber-Angriff auf ein Land, hinter welchem eine terroristische Organisation steckt, betitelt [85].

3.2. Datendiebstahl Aum Shinrikyo

Eine religiöse Vereinigung in Japan, die sich Aum Shinrikyo nennt, konnte Informationen zu einigen nuklearen Einrichtungen aus verschiedenen Standorten in mehreren Ländern beschaffen. Die gestohlenen vertraulichen Informationen konnten von der Polizei in Tokio im Hauptquartier der Gruppe, am Fuß des Fuji-Berges, beschlagnahmt werden. Die Polizei spricht von einem Cyber-Angriff auf die Computer der betroffenen Einrichtungen.
[101]

Angreiferin/Angreifer
Die religiöse Gruppierung Aum Shinrikyo (auch bekannt als Ōmu Shinrikyō beziehungsweise japanisch „オウム真理教“) ist der Drahtzieher hinter den Angriffen. In diesem Fall ist das ziemlich sicher, da die vertraulichen Informationen auf den Systemen von Aum Shinrikyo gefunden wurden und in mehreren Quellen der Angriff dieser Gruppierung eindeutig zugewiesen wird [86] [101] [102] [103]. Gründer und lange Zeit auch Anführer von Aum Shinrikyo war Matsumoto Chizuo, welcher sich aber Asahara Shōkō nannte [104]. Er ist unter anderem für die Anschläge in der Tokioter U-Bahn 1995 verantwortlich, für welche die Gruppe sehr bekannt ist [103] [104]. Asahara Shōkō wurde mittlerweile 2018 hingerichtet [104]. Seit 1997 ist die Gruppierung von den Vereinigten Staaten von Amerika als terroristisch eingestuft [8]. Heute wird die Gruppe unter dem neuen Namen Aleph fortgeführt und steht unter Beobachtung der japanischen Behörden [104].

Die Mitglieder von Aum Shinrikyo glauben, dass die Welt in Gut und Böse unterteilt ist und sie selbst ungeschätzte Avatare einer neuen Weltordnung sind [86]. Sie gehen davon aus, dass sie aktuell von den bösen Mächten in der Welt entkräftet werden [86]. Um ihre Macht wiederzuerlangen möchten sie die Apokalypse herbeiführen, da sie im folgenden Krieg ihre Feinde auslöschen wollen [86]. Die Apokalypse konnten sie allerdings mit ihren Anschlägen in der U-Bahn nicht auslösen. Durch das Hacken einiger nuklearer Einrichtungen, welche dann in einer nuklearen Katastrophe Landstriche verwüsten, würde jedenfalls ein sehr großer Schaden entstehen.

Ziel
Aum Shinrikyo konnte eine Vielzahl an Informationen von unterschiedlichen Zielen sammeln. Im Folgenden sind die Ziele und die damit verbundenen Informationen aufgelistet. Die religiöse Gruppierung hatte Informationen über

- ein von Russland in Auftrag gegebenes Gerät zur Verarbeitung von Plutonium [101],
- den schnellen Brutreaktor im japanischen Kernkraftwerk Monju [86],
- das Sicherheitssystem des Kernkraftwerks in Tschernobyl [101],
- das japanische Nuklearprogramm inklusive Kernbrennstofflieferanten und Transportrouten von Kernmaterial [86],
- sowie weitere Daten über kerntechnische Anlagen in Russland, der Ukraine, der Volksrepublik China, Südkorea und Taiwan [86] [101].

Jedoch behauptet das russische Atomenergieministerium, dass Aum Shinrikyo keine Informationen über russische Kernanlage haben kann [105]. Auch die Gruppe Aum Shinrikyo selbst äußerte sich zu den gefundenen Daten und ein Sprecher gab an, dass die Gruppe mithilfe der Daten nicht vorhatte eine nukleare Katastrophe auszulösen, sondern vielmehr die Informationen deshalb sammelte, damit sie besser auf Vorfälle in Atomkraftwerken reagieren können (Anmerkung: Diese Behauptung ist insofern nachvollziehbar, da die Gruppe legal bei den betroffenen Einrichtungen gearbeitet hatte. Weitere Informationen dazu finden sich im nächsten Abschnitt Angriff).

Angriff
Im Gegensatz zu anderen hier präsentierten Angriffen gelangte Aum Shinrikyo ohne Hacken der betroffenen Einrichtungen an die Informationen. Der Kult gründete mindestens fünf Computersoftwarefirmen mit insgesamt etwa 40 Mitarbeiterinnen und Mitarbeitern, die alle zu Aum Shinrikyo gehörten. Beispiele für diese Aum Shinrikyo Firmen sind Vainqueur Ltd. [102] [106] und Weinker [101]. Diese Firmen hatten etwa 190 Kundinnen und Kunden, welche allerdings nichts von der Verbindung der Computersoftwarefirmen zu Aum Shinrikyo wussten. Zu den Kundinnen und Kunden gehörten Firmen und staatliche Einrichtungen, darunter auszugsweise:

- Osaka Bank in Japan
- Universität in Tokio
- Verteidigungsministerium Japans
- Tokyo Metropolitan Police Department
- Nippon Telegraph and Telephone (kurz NTT)
- Honda
- Kyodo News

Viele der Kundinnen und Kunden gaben an, dass sie die Firmen vor allem deshalb schätzten, weil sie hochqualitative Systeme zu niedrigen Preisen lieferten. Durch den engen Bezug zwischen den Computerfirmen und Aum Shinrikyo wurden die Daten der betroffenen Kernanlagen auch für die Forscher von Aum Shinrikyo zugänglich.
[106]

Folgen
Grundsätzlich wurden in diesem Fall nur vertraulich eingestufte, geheime Informationen und Dokumente für unbefugte Personen öffentlich. Allerdings sprechen die behandelten Quellen nicht davon, dass Aum Shinrikyo die gesammelten Informationen außerhalb des eigenen Kults weiterveröffentlicht hätte. Dadurch blieben die Informationen zu den Kernanlagen weitestgehend unter Verschluss und nur Mitglieder von Aum Shinrikyo haben sie unbefugterweise einsehen können. Nachdem die Polizei in Tokio die Arbeiten von Aum Shinrikyo frühzeitig unterbrechen konnte, sind keine weiteren Schäden an den betroffenen Einrichtungen (siehe Abschnitt Ziel) entstanden.[10]

[10] Die Behauptung, keine weiteren Schäden seien an den Kernkraftanlagen entstanden sind, basiert auf den Informationen aus den Quellen [86] und [101] – [106].

3.3. Estland

In Estland fanden im Jahr 2007 Unruhen statt, welche von Cyber-Angriffen begleitet wurden. Als Auslöser und Grund für den Angriff auf Estland wird das Versetzen eines Monuments, das an die Befreiung Estlands während des zweiten Weltkrieges durch Russland erinnert, in Tallinn seitens der estnischen Regierung gesehen [107]. Das Monument, der „Bronze Soldat“, steht bereits seit 1947 in der estnischen Hauptstadt Tallinn [108]. Das Versetzen der Statue sorgte nicht nur für Aufstände seitens russischer Minderheiten [88], sondern auch für den Cyber-Angriff.

Estland war früher Teil der Sowjetunion und ist seit deren Zerfall 1991 unabhängig. Seltsam ist hierbei unter anderem, dass die Statue ziemlich lange von der freien estnischen Bevölkerung akzeptiert wurde und die Menschen sich erst relativ spät davon gestört fühlten [108]. Diesen Umständen soll hier aber nicht nachgegangen werden, allerdings beschäftigt sich der Autor aus [108] genau mit diesem Problem.

Angreiferin/Angreifer
Wer in folgendem Fall hinter dem Angriff steckt ist zumindest laut [87] und [88] nicht feststellbar. Die Ursache dafür wird in der Anonymität gesehen, welche das Internet bietet. Es gibt Spuren, die belegen, dass der Angriff von einem russischen Regierungscomputer stammt [109]. Die Autorin aus [109] ist weiters der Meinung, dass diese Involvierung eines Regierungscomputers nicht nur ein Anzeichen für Hacktivismus, sondern auch ein Anzeichen dafür ist, dass es sich nicht um eine einzige Angreiferin oder einen einzigen Angreifer mit großem technischen IT-Wissen handelt, sondern um viele Einzeltäterinnen und Einzeltäter, sogenannte „Script-Kiddies“, die bereits vorhandene Tools zum Ausnutzen von Schwachstellen verwenden. Unabhängig davon, ob es sich um einen Fall von Hacktivismus oder Terrorismus handelt, denn das ist nur reine Definitionssache, ist die Theorie eines weit verbreiteten Angriffs von mehreren Personen durchaus möglich. In russischen Foren wurden Anleitungen dazu gefunden, wie man die estnische Regierung angreifen und ihr schaden könne [87]. Auch die eher vernachlässigbaren Folgen und die Tatsache, dass Großteils Denial of Servie Angriffe gestartet wurden, sind laut [109] ein Anzeichen für die wenigen technischen Kenntnisse der Angreiferinnen und Angreifer.

Betrachtet man das ganze Geschehen allgemein von außerhalb, ist es naheliegend, dass die Cyberangriffe russischen Hackerinnen und Hackern zuzuschreiben sind. Außerdem sind die Unruhen und Aufstände ebenfalls von russischen Minderheiten verursacht wurden. Allerdings dementiert die russische Regierung irgendetwas mit den Angriffen zu tun zu haben [87]. Der Autor aus [87] ist davon überzeugt, dass diese Aussage stimmt, fügt aber noch hinzu, dass es zwar keine Beweise dafür gibt, dass die russische Regierung lügt und doch beteiligt ist, aber bei der Aufklärung des Falls wurde von russischer Seite keine Hilfe geleistet. Eine politische Motivation hinter dem Angriff lässt sich in Phrasen wie „ANSIP_PIDOR=FASCIST“ [87] erkennen. Andrus Ansip ist der Premierminister Estlands zum Zeitpunkt der Angriffe auf Estland. „Pidor“ kann als eine offensive Art einem nicht homosexuellen Mann als homosexuell zu bezeichnen [110] verstanden werden. „Fascist“ legt nahe Ansip als Faschisten beschuldigen zu wollen. Zusätzlich wurden auch andere ähnliche Phrasen mit obszönen und beleidigenden Inhalten gefunden [87]. Außerdem wurde auf den gehackten Seiten Estlands die falsche Nachricht verbreitet, dass der Premierminister und die Regierung die Russen um Verzeihung bitten und den Bronze Soldaten an seinen ursprünglichen Standort zurückbringen wollen [111].

Obwohl es Spuren gibt, die nach Russland führen [109], muss das nicht bedeuten, dass Russland nicht doch vollkommen unschuldig ist. Immerhin besteht die Möglichkeit, dass die Spuren gelegt sind und tatsächlich jemand anderer hinter dem Angriff steckt, der genau weiß, wie er den Angriff verschleiern kann. Diese Theorie wird beispielsweise in [87] gebracht. Der Autor [87] kommt aber selbst zu dem Schluss, dass das widersprüchliche an dieser Theorie die verweigerte Hilfe Russlands bei der Aufklärung des Falls ist. Eine zweite Theorie von [87] ist die „Grass Roots Response“ (Graswurzelbewegung/Basisbewegung). Sie besagt, dass es sich bei dem Angriff um einen groß angelegten internationalen Angriff auf die estnische Regierung handelt, der von der Bevölkerung ausgeht. Jedoch hält der Autor [87] selbst diese Theorie für noch unwahrscheinlicher als die erste, da es seiner Meinung nach eindeutige Spuren für staatliche Unterstützung gibt.

Im Zuge der Aufklärung des Falls konnten zwei Personen ausgemacht werden. Bei der ersten handelt es sich um Dmitri Galuškevitš [87] [112]. Galuškevitš war ein damals 20-jähriger Student aus Estland, welcher die Angriffe in Estland befindlich durchführte. Dadurch, dass er die Angriffe aus estnischen Netzwerken startete konnten genug Beweise für seine Beteiligung gefunden werden, was zu seiner Festnahme und anschließenden Verurteilung führte [87] [112].

Die zweite Person ist Konstantin Goloskokov. Er ist ein „Kommissar" der russischen Kreml-Jugend Naschi[11]. Die Kreml Jugend bekannte sich 2009 zu dem Fall und Goloskokov gab im Zuge dessen der Zeitung „Financial Times" ein Interview. Darin erläutert er, dass der Angriff nicht von der russischen Regierung beauftragt wurde, sondern die Gruppe aus eigener Initiative heraus handelte. Goloskokov nennt die Aktion keinen Cyber-Angriff, sondern eine Cyber-Verteidigung. Die estnische Regierung handelte aus ihrer Sicht illegal und man wollte ihnen eine Lehre erteilen. Das eigene Handeln der Kreml-Jugend bezeichnete Goloskokov hingegen nicht als illegal, da sie die betroffenen Internet-Seiten nur so oft besucht hätten, bis sie eben nicht mehr funktioniert haben. Um das zu erreichen wurden Privatpersonen ermutigt auf ihren eigenen PCs Tools auszuführen, die zu den Abstürzen der estnischen Regierungsseiten führten.
[113]

Die Kreml-Jugend Naschi ist privat finanziert, die Idee für diese Jugendorganisation stammt von Wladislaw Jurjewitsch Surkow. Die Vereinigung wurde 2003 von Wasili Jakemenko gegründet, ehe sie 2013 wieder aufgelöst wurde. Surkow und Jakemenko haben bereits eine gemeinsame Vergangenheit und gründeten bereits im Jahr 2000 eine regierungsfreundliche Jugendorganisation namens Iduschtschie wmeste[12].

Goloskokov gab an, dass der Angriff von Privatpersonen durchgeführt wurde. Aus dem Jahr 2007 existieren Statistiken zur Bekanntheit der Naschi in Russland und zur Einstellung der Bevölkerung gegenüber dieser Bewegung. Daraus geht hervor, dass etwa 34% wissen, dass es die Organisation gibt, aber eine positive Einstellung haben nur etwa 10% der Bevölkerung. Es ist fraglich, wie viele Personen die Kreml-Jugend tatsächlich zu einem Angriff bewegen konnte, aber bei einer Bevölkerung Russlands von 143 Millionen im Jahr 2007 [114] könnten im besten Fall 14 Millionen Personen allein in Russland am Angriff teilgenommen haben. Hierbei müssten allerdings noch Personen ohne PC-Zugang und Personen, die nicht davon gehört beziehungsweise aus anderen Gründen nicht am Angriff teilnehmen konnten und wollten abgezogen werden. Die tatsächliche Beteiligung dürfte allerdings nicht zu hochgewesen sein, da lediglich eine Internetauslastung von 100 Megabyte pro Sekunde [113] in estnischen Netzwerken herrschte. Auch für 2007 ist das nicht gerade viel, da laut Aussage eines Experten [113] der größte Angriff bis zu den Ereignissen in Estland eine Auslastung von 40 Gigabyte pro Sekunde verursachte.
[115]

Offiziell bekannt hat sich die Kreml Jugend Naschi zwar, eindeutige Nachweise dafür gibt es allerdings nicht. Deshalb stellt sich die Frage, wie realistisch es ist, dass diese Bewegung der Hauptakteur hinter den Angriffen ist. Basierend auf den vorliegenden Fakten zu dem Fall, ist es am wahrscheinlichsten, dass hauptsächlich Russinnen und Russen von Sympathisantinnen und Sympathisanten der russischen Regierung, wie den Naschi und möglicherweise anderen Organisationen dazu ermutigt wurden einfache Skripte auf ihren Privatrechnern auszuführen, die die Infrastruktur Estlands lahmlegen. Offenbar war die Teilnahme der Bevölkerung nicht so zahlreich wie ursprünglich erhofft, aber dennoch wirksam, da Estlands Infrastruktur schlecht aufgebaut war und schon bei einer eher geringen Auslastung den Dienst verweigerte. Dadurch erklären sich auch Spuren, die nach Russland führen, aber keiner Organisation eindeutig zuzuschreiben sind. Obwohl zwar eindeutig Schäden für Estland entstanden sind (siehe Abschnitt Folgen) ist nur anhand der Fakten allerdings schwer abzuschätzen inwiefern man Estland tatsächlich schaden wollte.

[11] Das Wort stammt aus dem russischen, wird original „Наши" beziehungsweise „Naši" geschrieben, und bedeutet zu Deutsch „Die Unseren"
[12] Zu Deutsch: „Gemeinsam gehen"

Ziel

Bei den Angriffen auf Estland gab es kein einzelnes Ziel, vielmehr wurde eine Vielzahl an Regierungssystemen, aber auch regierungsunabhängigen Systemen von Firmen, die in Estland geschäftstätig sind, angegriffen. Zu den Zielsystemen gehörten:

- Webserver
- E-Mail-Server
- DNS-Server
- Router

Für die Öffentlichkeit waren hierbei vor allem die Angriffe auf Webserver sichtbar. Die betroffenen Assets gehörten, wie eingangs erwähnt, verschiedenen Besitzern. Dazu zählen:

- Regierung Estlands
- Premierminister Estlands (Im Jahr 2007 Andrus Ansip)
- Parlament Estlands
- Polizei Estlands
- 2 Banken
- Internet Service Provider
- Online Medien
- Viele Kleinunternehmen
- Lokale Regierungen
- Politische Parteien

[87] [88]

Warum Estland generell von Unruhen betroffen war, ist auf das Versetzen des Bronze Soldaten zurückzuführen [87] [88] [108]. Dadurch bleibt nur noch die Frage offen, warum ein Cyber-Angriff stattgefunden hat. Estland war 2007 in Asien und Europa von allen Ländern auf Platz 20 bezüglich der IT Infrastruktur platziert und ragte für die erheblichen Fortschritte, die es in den letzten Jahren gemacht hatte aus der Masse heraus [116]. Auch die Autorin aus [117] beschreibt Estland 2007 als ein sehr fortschrittliches Land bezüglich Internetabdeckung und -verfügbarkeit. Estland führte beispielsweise als erstes Land ein nationales Wahlsystem über das Internet ein, welches im Februar 2007 vor den Cyberangriffen zum Einsatz kam [117]. Zusätzlich waren bereits 2007 kritische Infrastrukturen Estlands vom Internet abhängig [88]. Dazu zählen neben den Regierungsgeschäften auch die Stromnetze und die Stromversorgung, Bankservices, sowie die Wasserversorgung der Hauptstadt Tallinn [88].

Wenn man diese Automatisierung und Vernetzung erfolgreich angreift, verursacht das sehr hohe Schäden und legt einen Großteil des Landes lahm, was auch passiert ist (siehe Abschnitt Folgen). Da Estland in öffentlichen Reports und Artikeln, wie in [116], als fortschrittlich erwähnt wurde und Ereignisse wie die nationale Wahl über das Internet sich herumgesprochen haben müssen, konnte beispielsweise die Kreml-Jugend Naschi leicht darauf aufmerksam werden, dass hier ein potenzielles Ziel liegt.

Der Chef der IT-Sicherheit, Mihkel Tammet, aus dem Verteidigungsministerium Estlands gab in einem Interview [111] an, dass man sich der hohen Abhängigkeit eines funktionierenden Netzwerks und Internets bewusst war. Diese Abhängigkeit sah er vor allem in der „papierlosen Regierungsarbeit“ und dem webbasierten Banking [111]. Als Gegenmaßnahme für die Angriffe wurde versucht den Zugriff auf betroffene Webseiten und Services für Externe vorübergehend zu sperren, während man gleichzeitig für Benutzer innerhalb Estlandes die Services weiterhin verfügbar halten wollte [87] [111]. Generell wurde von offizieller Seite des Verteidigungsministeriums von terroristischen Aktivitäten gesprochen [111].

Angriff

Grundsätzlich kamen bei den Angriffen hauptsächlich Methoden zum Einsatz, die einen Denial of Service beziehungsweise einen Distributed Denial of Service der estnischen IT-Infrastruktur verursachten. Es handelte sich um folgende Angriffe:

- ICMP Flooding (Überfluten des Zielsystems mit Internet Control Message Protocol Echo Anfragen)
- UDP Flooding (Überfluten des Zielsystems mit User Datagram Protocol Paketen, damit dieses mit der Verarbeitung überfordert ist und nicht mehr antworten kann)
- Manipulierte Webanfragen
- E-Mail Spam (Offizielle Regierungsadressen sendeten zahlreiche Mailnachrichten

[118]

In russischen Foren gab es Anleitungen dazu, wie man diese Angriffe ausführt, wie beispielsweise in Abbildung 8: Russische Anleitung [87] (Zur besseren Verständlichkeit der Abbildung ist eine deutsche Version dieses Textes in Abbildung 9: Übersetzung von Abbildung 8 vorhanden) sichtbar ist. Personen, die sich dazu entschieden an den Angriffen an der estnischen IT-Infrastruktur teilzunehmen brauchten daher nicht sehr gute IT-Kenntnisse, da sie mithilfe solcher Anleitungen Unterstützung bekamen.
[87]

Es gab auch komplexere Angriffsmethoden wie SQL-Injektionen, welche allerdings nur nicht kritische Infrastruktur und nicht kritische Web Server erfolgreich manipulieren konnten [87]. Normalerweise erhielten die estnischen Regierungsseiten etwa 1000 Besuche pro Tag, während der Angriffe wurden es jedoch 2000 Aufrufe pro Sekunde [119]. Die Netzauslastung betrug wie vorab schon erwähnt etwa 40 Megabyte [113]. Der Großteil der Angriffe kam von außerhalb Estlands, die meisten davon stammen von russischen IP-Adressen [87].

Durch die Versetzung des Bronze Soldaten starteten die allgemeinen Unruhen am 27. April 2007 und dauerten bis 18. Mai 2007 an. In der Nacht vom 8. Mai auf den 9. Mai erreichten die Cyber-Angriffe dabei einen Höhepunkt. Der Autor aus [87] sieht darin ein besonderes Datum für Russland, da an diesem Tag der Sieg über das nationalsozialistische Deutschland gefeiert wird. Schließlich wurde Estland neben einigen anderen Ländern, von den Russen befreit, das aber schon etwas früher im Jahr 1944 [120]. Immerhin erinnert aber der versetzte Bronze Soldat an die gefallenen Soldaten von damals [108] und wäre damit ein weiterer Hinweis dafür, dass Russland in die Geschehnisse involviert ist, wenn man mit dem neuen Platz für das Monument nicht zufrieden war. Auch die Aufforderung zum Angriff auf estnische Services in Abbildung 8 erwähnt den 9. Mai.
[87]

Der Autor aus [118] spricht von 2 Phasen, in welchen der Angriff stattgefunden hat. Die erste Phase vom 27. April 2007 bis 29. April sieht er als emotionale Reaktion nach der Entscheidung den Bronze Soldaten zu versetzen. Diese ersten Denial of Service Angriffen waren nicht sonderlich organisiert und auch nicht so weitreichend und verbreitet wie jene in der zweiten Phase [112]. Die zweite Phase vom 30. April bis 18. Mai bezeichnet [118] als Hauptangriff. Dieser war weit besser organisiert, als die ersten Angriffe und erreichte auch größere Dimensionen. Dadurch starteten Distributed Denial of Service Angriffe, Webseiten wurden manipuliert und viele E-Mail Spam Nachrichten wurden verschickt [112].

На 9-е МАЯ планируется повтор данной акции!
Не дай унизить своих соотечественников, отомсти за издевательства !!!
@ адреса eSStонских депутатов

Программа для рассылки писем
(пароль на RAR: nnm)

Нажми (**пуск -> выполнить -> cmd**)
Введи **ping - 5000 - 10000 эSStонский_сайт -t** и жми **ENTER** ВСЕ !!! Твои пламенные приветы полетели...
пример: **ping - 5000 - 1000 www.riik.ee -t**
Это 3 элементарных действия, после которых многие эстонские сайты просто перестанут работать!!!
Или вот .BAT файл, который в автоматическом режиме последовательно пингует эстонские DNS и MAIL сервера. Цикл бесконечен :)
Скопировать (красным) нижеприведённый текст, вставить в блокнот и сохранить как **privetesStonia.BAT** (название можно любое) файл
(ты можешь сам добавлять адреса)

Abbildung 8: Russische Anleitung [87][13]

Am 9. Mai ist eine Wiederholung dieser Aktion geplant!
Lass deine Landsleute nicht demütigen, räche Mobbing !!!
@ adressen von eSStnischen Abgeordneten

Programm zum Versenden von E-Mails
(*Passwort auf RAR: nnm)*

Drücke (**Start -> Ausführen -> cmd**)
Gib **ping - 5000 - 10000 eSStnische_seite -t** ein und drücke **ENTER** ALLE !!! Deine feurigen Grüße folgen ...
Beispiel: **ping - 5000 - 1000 www.riik.ee -t**
Dies sind 3 grundlegende Aktionen, nach denen viele estnische Websites einfach nicht mehr funktionieren!!!
Oder hier ist eine .BAT-Datei, die estnische DNS- und MAIL-Server automatisch anpingt. Der Zyklus ist endlos :)
Kopiere den untenstehenden Text (rot), füge ihn in den Editor ein und speichern ihn als **privetesStonia.BAT** (beliebiger Name) Datei
(Du kannst Adressen selbst hinzufügen)

Abbildung 9: Übersetzung von Abbildung 8

[13] Zur besseren Lesbarkeit handelt es sich bei der Abbildung um eine Transkription inklusive Adaption des originalen Bildes aus [87]. Die deutsche Übersetzung von Abbildung 9 erfolgte mithilfe von https://translate.google.com/.

Folgen

Die Cyber-Angriffe hatten sowohl wirtschaftliche als auch gesellschaftliche Auswirkungen. Nicht nur große Unternehmen, die Regierung, Banken und Medienunternehmen waren für ihre Geschäfte auf eine funktionierende Informations- und Kommunikations-Infrastruktur angewiesen, sondern auch Klein- und Mittelunternehmen [121]. All diese Unternehmen konnten ihre Geschäfte nicht mehr wie gewohnt fortführen und mussten daher wirtschaftliche Einbußen verzeichnen [118]. Manche Webseiten waren hierbei nur eine halbe Stunde unerreichbar, andere aber bis zu mehreren Stunden [122].

Gesellschaftliche Auswirkungen waren vor allem dadurch spürbar, weil man in es Estland bereits gewohnt war Informationen überall online abzurufen. Nachdem die offiziellen Webseiten der Regierung von der Bevölkerung für verschiedenste Zwecke genutzt wurden, welche beispielsweise das Einreichen von Steuerberichten, Beantragen von staatlichen Leistungen und Zuschüssen umfassen, ergaben sich für betroffene Personen finanzielle Schäden. Die offizielle Kommunikation mit der Regierung wurde auch durch den E-Mail-Spam lahmgelegt. Allgemein ist es schwer zu sagen, welcher Schaden für die Bevölkerung entstanden ist. Die Schäden reichen hier von einfachen Unannehmlichkeiten, Umständlichkeiten und Verzögerungen bis hin zu materiellen Verlusten und Schäden.
[118]

Während der Angriffe wurde als eine der Gegenmaßnahmen die Erreichbarkeit estnischer Seiten beschränkt [87]. Zunächst begannen beispielsweise Banken damit die Webseiten und Services nur innerhalb Estlands verfügbar zu machen, weiteten dies aber dann auf andere Länder aus, welche keine oder nur sehr wenige vernachlässigbare Angreifer, aber viele Kunden hatten [87]. Im Bezug zu den Auswirkungen auf die Bevölkerung bedeutet dies aber, dass die betroffenen Kunden dieser Banken dann nicht nur durch die Terroristinnen und Terroristen vom Zugriff abgehalten wurden, sondern auch von Estland selbst.

Die Angriffe hatten auch Einfluss auf den Informationsfluss und die Berichterstattung aus Estland. Die estnische Regierung verbreitet Informationen weitestgehend online an internationale Medien. Diese Medien hatten keine Vertreterinnen, Vertreter oder andere Berichterstatter in Estland, was dazu führte, dass der Informationsfluss von der estnischen Regierung an lokale und internationale Medien beeinträchtigt wurde. Tatsächlich gehörten diese Regierungsseiten, welche zum Verbreiten von Informationen genutzt wurden, zu den ersten Zielen der Cyber-Angriffe.
[118]

Einen sehr guten Einblick in die Geschehnisse und dessen Auswirkungen in Estland bieten die Schilderungen von Sami Saydjari aus [123], einem Experten für Cyber Defense. Dieser schilderte die Ereignisse im April 2007 vor einem Komitee für Heimatschutz. Dabei sprach er von gestörten Kommunikationsmitteln, nicht funktionierenden Internetverbindungen, sowie davon, dass Geldautoamten und Ampeln in ihrer Funktion gestört waren. Weiters sind Radio- und Fernsehübertragungen nicht mehr möglich gewesen und Flughäfen und Bahnhöfe hatten den Betrieb eingestellt. Dazu kommt noch, dass selbst die Produktion von Nahrungsmitteln angehalten wurde und auch die Wasserversorgung aufgrund der nicht mehr funktionierenden Pumpen nicht mehr sichergesellt war. Dies führte zu Panik in der Öffentlichkeit und Plünderungen, die von der Polizei nicht mehr kontrolliert werden konnten.
[123]

Trotz der großen Erfolge, welche die Angreiferinnen und Angreifer erreichen konnten, wurde der Bronze Soldat nicht wieder an seinem ursprünglichen Standort im Stadtzentrum Tallinns aufgestellt. Er steht bis heute an seinem neuen Platz im Tallinna Kaitseväe kalmistu (in englischer Sprache bekannt als „Defence Forces Cemetary“, zu Deutsch: „Friedhof der Verteidigungskräfte“).
[124]

3.4. Georgien

Im Zuge des Krieges zwischen Russland und Georgien im Jahr 2008 fanden neben dem militärischen Konflikt einige Cyber-Angriffe auf das Land Georgien statt. Der militärische Krieg startete am 7.August 2008 und dauerte nur etwa eine Woche an. Er ist ein Resultat eines längeren Streits zwischen Russland und Georgien um Regionen im Kaukasus. Dazu kommen rechtliche, kulturelle und wirtschaftliche Faktoren, aber auch die vorausgehenden Kriege 1992 und 1993, die zum Konflikt 2008 führten.
[89]

Angreiferin/Angreifer
Da die Cyber-Angriffe im Zeitraum um den Krieg mit Russland passierten, ist es sehr wahrscheinlich, dass sie von Russland ausgehen. Bestätigt wurde das von russischer Seite nicht, vielmehr wurden sämtliche Anschuldigungen immer dementiert [125]. In Georgien ist man davon überzeugt, dass die Angriffe von Moskau ausgehen, nur kann das von georgischer Seite nicht bewiesen werden [125]. Tatsächlich gibt es Beweise die neben dem Konflikt zwischen Russland und Georgien den Verdacht auf Hackerinnen und Hacker aus Russland erhärten. Im Zuge von Aufklärungsarbeiten konnte man in russischen Hacker-Foren Posts zu den Angriffen auf Georgien finden [126]. Für diese Arbeiten wurden die Foren xakep.ru und stopgeorgia.ru, sowie Daten des georgischen Netzwerkservers untersucht und insgesamt 200 Posts analysiert [126].

Obwohl es keine Beweise für einen direkten Einfluss der russischen Regierung auf diese Hackerinnen und Hacker gibt [126], spielen die Angriffe dieser sehr stark mit den Ereignissen des Krieges zusammen. Bei den Angriffen auf die Stadt Gori beispielsweise wurden nur kurz vor dem Angriff der russischen Luftwaffe offizielle Internetseiten und Nachrichtenseiten von den Hackerinnen und Hackern abgeschalten [89]. In [126] ist man der Ansicht, dass die russische Regierung sehr wohl passive Unterstützung für die Hackerinnen und Hacker leistete und versuchte von ihren Angriffen zu profitieren. In der Vergangenheit haben russische Regierungsmitglieder bereits solche Hacker-Gruppen unterstützt [126]. Schließlich geht man noch aufgrund der Komplexität mancher Angriffe davon aus, dass einige der Hackerinnen und Hacker sehr gute technische Kompetenz aufweisen [127]. An anderer Stelle waren die Angriffsversuche sehr schlecht umgesetzt [90], was bedeuten könnte, dass hier sehr viele Personen mit unterschiedlichen Fähigkeiten zusammengearbeitet haben.

Ziel
Die Angriffe waren nicht auf ein einzelnes Unternehmen oder ausschließlich die Regierung gerichtet. Sie waren teilweise mit den Angriffen des russischen Militärs kombiniert und teilweise eigenständig. Dadurch wurden unterschiedliche Ziele in Georgien Opfer von den Angriffen. Eine Liste der geplanten Ziele findet sich in Tabelle 11: Angriffsziele laut www.StopGeorgia.ru [128]. Bei www.StopGeorgia.ru handelt es sich um eines der Foren, welches die Angreifer zum Informationsaustausch nutzten (siehe auch Abschnitt Angreifer).

In Tabelle 11 wird in der Spalte Betroffenes Ziel der Betroffene beziehungsweise die laut [128] angegebene Beschreibung des Betreibers angegeben. Falls das Ziel eine Webseite betreibt, die ein Ziel darstellt, wird diese in der Spalte Webseite angegeben. In der Spalte Anmerkungen befinden sich bei Bedarf zusätzliche Informationen zum betroffenen Ziel und den verbundenen Umständen aus [129]. Keine Anmerkung bedeutet, dass die Seite laut [129] von Störungen im Zeitraum zwischen 13. und 24. August 2008 betroffen war.

Allgemein gesehen war Georgien zur Zeit des Krieges ein Nachzügler, was die Anbindung der Bevölkerung an das Internet betrifft. Nur etwa 10% der Bevölkerung nutzte das Internet. 175 000 Menschen (4% der Bevölkerung) hatten einen Festnetzanschluss, während 2,7 Millionen Personen (62% der Bevölkerung) zumindest über ihre Mobiltelefone die Möglichkeit hatten auf das Internet zuzugreifen. Hinzu kommt noch, dass im Jahr 2008 Georgiens Zugang zum Internet sehr stark von der russischen Netzinfrastruktur abhängig war, wodurch Russland zusätzlich leichter die Verbindung Georgiens stören konnte.
[90]

Betroffenes Ziel	Webseite	Anmerkungen
Georgischer Präsident [90]	-	Diese Angriffe fanden im Juli 2008, vor der kriegerischen Auseinandersetzung im August, statt.
Internet Service Provider Georgiens [90]	-	
Hacker Forum Georgiens	-	Eines der ersten Ziele, um Gegenschläge zu vermeiden [130].
Parlament	www.parliament.ge	
Goskomstat	www.assistancegeorgia.org.ge	
Wahlkommission	www.cec.gov.ge	
Stadtentwicklungsfonds	www.mdf.org.ge	
Außenministerium	www.mfa.gov.ge	
Anti-Korruptionsprogramm	www.corruption.ge	
Verfassungsgericht	www.constcourt.gov.ge	
Versicherung	www.insurance.caucasus.net	
Kulturministerium	www.mc.gov.ge	
Sicherheitsrat	www.nsc.gov.ge	
Oberster Gerichtshof	www.supremecourt.ge	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
Verkehrsministerium	www.iberiapac.ge	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
Department of material service[14]	www.court.gov.ge	
Vereinte Nationen in Georgien	www.civil.ge	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
Botschaft der Vereinigten Staaten in Tiflis	georgia.usembassy.gov	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
Botschaft des Vereinigten Königreichs in Tiflis	ukingeorgia.fco.gov.uk/en	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
-	all.ge	
-	geres.ge	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
Fernsehkanal	www.rustavi2.com	
Elektronische Versionen von Zeitungen	www.opentext.org.ge	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
Zeitung Свободная Грузия (Freies Georgien)	www.svobodnaya-gruziya.com	
Zeitung Georgian Times	www.sanet.ge/gtze	
Zeitung Georgian Messenger	www.messenger.com	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
Agentur Прайм-ньюс (Prime News)	www.primenewsonline.com	
Nachrichtenagentur	www.presidpress.com	
Werden in [128] neben anderen besser beschriebenen Webseiten unter dem Abschnitt Medien geführt.	www.sakinform.ge	
	www.sakartvelo.ru	
	www.internews.ge	
	www.internews.org.ge	
	www.interpressnews.ge	
-	www.internet.ge	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].

[14] Originalbegriff verwendet in [128]

Fernsehnachrichten	www.stream.ge	
-	newsgeorgia.ge	Keine Statusinformation von [129].
-	presa.ge	Nicht von Ausfällen oder anderen Einschränkungen betroffen [129].
-	www.medianews.ge	

Tabelle 11: Angriffsziele laut www.StopGeorgia.ru [128][15]

Angriff
Der Großteil der Angriffe bestand aus Denial of Service beziehungsweise Distributed Denial of Service Angriffen. Bereits vor dem Ausbruch des Krieges im August wurde im Juli die Webseite des georgischen Präsidenten mithilfe eines Distributed Denial of Service Angriffs für 24 Stunden unerreichbar gemacht [90]. Ebenfalls im Juli wurden Internet Service Provider in Georgien durch Distributed Denial of Service Angriffe dazu gezwungen ihre Services vorübergehend einzustellen [90].

Im August schließlich wurde der Umfang der Distributed Denial of Service Angriffe stark erhöht. Das für die Angriffe eingesetzte Botnetzwerk im August umfasste die IP-Adressen von 3 237 Computern aus insgesamt 62 Ländern. Die meisten davon stammten aus Deutschland (619) und den Vereinigten Staaten (597). Erst an dritter Stelle folgte Russland selbst mit 526 registrierten IP-Adressen. Eine Untersuchung, von wo aus die Command & Control Server der Botnetze gesteuert wurden verlief negativ. Die Server sind geografisch viel zu stark verstreut, um Rückschlüsse ziehen zu können von wo aus die Angriffe koordiniert wurden.
[131]

Zum Zeitpunkt des Kriegsbeginns im August kamen neben den Denial of Service Angriffen auch SQL-Injektionen und Cross-Site Scripting zum Einsatz. Diese wurden dazu verwendet das Aussehen der georgischen Seiten zu verändern, welche dann beispielsweise Adolf Hitler mit dem georgischen Präsidenten in ähnlichen Posen zeigten. Weitere Angriffe zielten darauf ab Malware auf den georgischen Systemen zu verbreiten. Diese Angriffe waren allerdings vergleichsweise wenig erfolgreich. Die Ursache dafür liegt in der Einfachheit der Malware und den schlecht gestalteten Spam E-Mails, welche die Empfänger sofort als Angriffsversuch erkennen konnten. Dadurch blieben Malware-Schäden weitestgehend aus oder waren nicht von langer Dauer.
[90]

Einige kritische Infrastrukturen waren zur Zeit der Hacker-Angriffe auf Georgien über das Internet erreichbar und boten somit potenzielle Ziele für die Angreiferinnen und Angreifer. Allerdings wurden diese weder von den Hackerinnen und Hackern noch vom russischen Militär angegriffen und es entstand kein Schaden. Dies könnte ein Hinweis darauf sein, dass auf russischer Seite jemand dafür sorgte die Angriffe einzuschränken. Es ist weiters auszuschließen, dass diese Einrichtungen verschont blieben, weil sie zu gut abgesichert waren, da die Angreiferinnen und Angreifer bei den anderen Zielen bewiesen haben wozu sie fähig sind.
[127]

Folgen
Die größten Auswirkungen hatte der Ausfall der zwei großen georgischen Internet Service Provider United Telecom of Georgia und Caucasus Network Tbilisi. Aufgrund der Angriffe konnten diese Provider ihre Dienste nicht mehr zur Verfügung stellen und somit schlussendlich keinen Internetzugang für die georgische Bevölkerung bereitstellen. Nachdem aber nur ein geringer Anteil der Bevölkerung die Internetdienste zu dieser Zeit nutzte, waren die schlussendlichen Schäden eher gering. Die Cyber-Angriffe verursachten allerdings finanzielle Schäden für die Betroffenen. Eine Schätzung der Kostenhöhe ist durch den Krieg aber schwierig.
[90]

[15] Bei den angegebenen Zielen unter „Betroffenes Ziel“handelt es sich teilweise um Übersetzungen von StopGeorgia.ru, die mithilfe von translate.google.com übersetzt wurden. Alle Ziele, die eine Quelle enthalten stammen aus dieser Quelle und wurden nicht mit translate.google.com übersetzt.

3.5. Infrastruktur Vereinigte Staaten[16]

Im April 2009 wurden Informationen veröffentlicht, wonach die Stromversorgung der Vereinigten Staaten von Schadsoftware betroffen war. Zwei ehemalige Beamte gaben in einem Interview an, dass der schädliche Code bereits 2006 oder 2007 entdeckt worden war. Neben den Systemen der Stromversorgung waren auch noch andere Infrastrukturen betroffen.
[132]

Angreiferin/Angreifer
Von Seiten der Vereinigten Staaten werden Russland und China beschuldigt hinter den Angriffen zu stehen, beziehungsweise sie in Auftrag gegeben zu haben. Ferner vermutet man eine Cyberspionage-Kampagne hinter den Angriffen [91], welche darauf abzielte die IT-Infrastruktur zu kartieren. Die Anschuldigungen, dass China oder Russland verantwortlich sind, wurden sowohl von russischer als auch chinesischer Seite zurückgewiesen [91]. Von russischer Seite distanzierte man sich nicht nur von den Angriffen auf die Infrastruktur der Vereinigten Staaten, sondern auch von allen anderen Angriffen, die in jedem anderen Land der Welt stattfanden [91]. Das ist insofern bemerkenswert, da man sich dadurch grundsätzlich auch von den Angriffen auf Estland (siehe Kapitel 3.3 Estland) und Georgien (siehe Kapitel 3.4 Georgien) nochmals distanziert, die aber durchaus Spuren aufweisen, die nach Russland führen. Diese beiden Fälle liegen zum Zeitpunkt der Veröffentlichung der Informationen zu den Angriffen auf die Stromversorgung in den Vereinigten Staaten nur etwa ein Jahr beziehungsweise zwei Jahre zurück. Von chinesischer Seite wurde von Gesetzen gesprochen, die derartige Angriffe verbieten und man bot zudem an, in Zukunft bei der Aufklärung derartiger Fälle zu helfen [91].

Ziel
Der Angriff richtete sich nicht gezielt an einen Stromversorger oder eine Region, sondern verbreitete sich im ganzen Land [91]. Außerdem waren nicht nur Stromversorger, sondern auch andere Betreiber von Infrastrukturen betroffen. Vielmehr finden sich Informationen über Schadsoftware bei Betreibern folgender Bereiche:

- Stromversorgung
- Wasserversorgung [91]
- Abwasseranlagen [91]
- Öl- und Gaslieferanten [132]
- Telekommunikationsfirmen [132]
- Finanzdienstleistungen [132]

Angriff
Grundsätzlich wurde der eigentliche Angriff nie gestartet. Zumindest wird seitens des Departments für Homeland Security [132] angegeben, dass es einen tatsächlichen Breach nie gegeben habe. Sollte es sich tatsächlich nur um eine reine Spionage, ohne Störungsabsichten handeln, wäre klar, wieso es zu keinen Ausfällen gekommen ist.

Eine andere Möglichkeit ist, dass man seit 2006 beziehungsweise 2007 ständig daran gearbeitet hatte, den Schadcode zu identifizieren und zu beseitigen, während die Angreiferinnen und Angreifer an anderer Stelle versuchten in die Systeme einzudringen. In einem derartigen Wettkampf gelang es allerdings den Angreiferinnen und Angreifern nie die Oberhand zu gewinnen und daher blieb auch der Angriff aus. Von offizieller Seite wurde damals gewarnt, dass die Angreiferinnen und Angreifer sehr wohl in der Lage gewesen wären Ausfälle der

[16] Die Datumsangabe 2009 bezieht sich auf das Bekanntwerden des Falls. Den ungefähren Angaben zweier Beamter zufolge [132] wurde der schadhafte Code bereits 2006 oder 2007 entdeckt. Dadurch ist anzunehmen, dass die Malware irgendwann vor diesem Zeitpunkt in die Systeme eingeschleust worden sein muss. Nachdem schwer zu sagen ist, seit wann betroffenen Infrastrukturen tatsächlich kompromittiert wurden, wurde als Jahr der Zeitpunkt der Bekanntgabe durch [91] gewählt.

betroffenen Infrastrukturen zu verursachen [91]. Man ging davon aus, dass diese Schadsoftware in diversen Infrastrukturen der Vereinigten Staaten deshalb platziert wurde, um sie bei Bedarf einzusetzen [91]. Dadurch hätte man beispielsweise im Kriegsfall als Angreiferin oder Angreifer die Möglichkeit die betroffenen Systeme abzuschalten und verschafft sich damit einen Vorteil [91]. Das gleiche gilt auch für Terroristinnen und Terroristen, wenn sie im Zuge eines größeren Anschlags zusätzlich Cyber-Angriffe durchführen. Selbst wenn keine der Möglichkeiten zutrifft, könnte jede dieser Varianten einen Vorteil für Supermächte wie Russland und China für diverse Situation bringen.

Folgen
Es sind keine Unterbrechungen oder andere Störungen an der Stromversorgung, welche durch diese Angriffe verursacht wurden, bekannt [132]. Allerdings kann ein Stromausfall in den Vereinigten Staaten Folgen haben, wie bereits beispielsweise 2003 deutlich wurde [133]. Damals waren 21 Kraftwerke ausgefallen und etwa 50 Millionen Menschen wurden zwischen zwei Stunden und mehr als einem Tag nicht mit Strom versorgt [133].

3.6. Saudi-Arabische Webseiten

Die Syrian Electronic Army verübte einige Hacker-Angriffe auf verschiedene Ziele in der Zeit zwischen 2011 und 2015 [134]. In diesem Fall soll beispielhaft ein Angriff von 2014 aufgearbeitet werden, in welchem die Syrian Electronic Army einige saudi-arabische Webseiten gehackt hat. Dieser Fall wurde ausgewählt, weil er sich gegen den saudi-arabischen Staat richtete und nicht wie viele andere Angriffe gegen Unternehmen [134].

In einem Statement 2014 beschuldigte die Syrian Electronic Army zunächst den saudi-arabischen Geheimdienst dessen, dass sie in Verbindung mit den Terroristinnen und Terroristen der Al-Qaida stehen und diese unterstützen [94]. Aus diesem Grund hackten sie 17 Seiten der saudi-arabischen Regierung, welche dann nicht mehr erreichbar waren [95] [135].

Angreiferin/Angreifer
Die Syrian Electronic hat sich in ihrem Statement ganz klar zu dem Fall bekannt und auch einen Grund angegeben [94]. Beides ist nachvollziehbar und somit kann mit sehr großer Wahrscheinlichkeit auch davon ausgegangen werden, dass die Syrian Electronic Army tatsächlich für die Angriffe verantwortlich ist. Jedoch bleibt noch zu klären wer die Syrian Electronic Army eigentlich ist. Auf ihrer eigenen Webseite „sea.sy“, die mittlerweile nicht mehr erreichbar ist (Stand der verwendeten Momentaufnahme von [136] ist der 13. März 2014), findet sich eine Beschreibung darüber, wie sie entstanden ist und worin sie ihren Zweck sieht [136]. Darin heißt es: „The SEA was created in 2011 when the Arab media and Western started their bias in favor of terrorist groups that have killed civilians, the Syrian Arab Army and have destroyed private and public property. […] “ [136]. Sie selbst bezeichnen sich als „[…] A group of young Syrians, not belonging to any governmental entity […]“ [136].

Die Homepage sea.sy bietet zudem geringfügig Informationen über die Mitglieder der Syrian Electronic Army. Großteils handelt es sich um Pseudonyme und den dazugehörigen Funktionen der einzelnen Mitglieder [136]. Bei einigen gibt es allerdings so gut wie keine Details [136]. Es lässt sich lediglich entnehmen, dass eine Aufgabenverteilung besteht und zehn Personen im ungefähren Zeitbereich der Angriffe Mitglieder bei der Syrian Electronic Army waren.

Die Hacktivisten-Gruppe Anonymus gab in einem Interview im September 2013 [137] an, dass sie Informationen darüber gefunden hätten, wer die tatsächlichen Personen hinter der Syrian Electronic Army beziehungsweise den Pseudonymen sind. Wirklich veröffentlicht haben sie die Information damals nicht, vielmehr wurden nur Hinweise auf die mutmaßlichen Akteurinnen und Akteure gegeben. Demnach kommen einige der Mitglieder aus Rumänien und Russland [137]. Im Mai 2018 schließlich wurden zwei ehemalige Mitglieder der Syrian Electronic Army von den Vereinigten Staaten unter anderem wegen Verunstaltungen an Webseiten angeklagt [138]. Bei den zwei Männern Ahmad ‘Umar Agha (Bekannt als „Th3Pr0“ aus [136]) und Firas Dardar (Bekannt als „The

Shadow“ aus [136]) handelt es sich allerdings um Syrer [138] und nicht um Rumänen oder Russen wie in [137] angegeben. Allerdings würden laut Angaben in [136] noch acht Personen fehlen.

Damit bleibt noch zu klären, ob und welche Verbindungen es zwischen der Syrian Electronic Army und der syrischen Regierung gibt. Auch dafür hat Anonymous einige Hinweise gefunden [137]. Demnach haben die Anführer der Syrian Electronic Army nicht nur Verbindungen zu Assad (Bashar al-Assad ist der Präsident Syriens zum Zeitpunkt des Cyber-Angriffs 2014) und der Regierung Syriens, sondern auch zu den Vereinigten Staaten [137]. In einem weiteren Statement (vergleiche mit dem obigen Zitat „A group of young Syrians[…]“ [136]) im Abschnitt „Funding“ [136] distanzieren sich die Mitglieder nochmals zur syrischen Regierung und möglichen anderen Organisationen: „Whatever is said, we, at the Syrian Electronic Army, assert we rely on self-funding from because our work only requires access to a computer line, Internet and set targets for the attacks or to publish the truth about the Syrian crisis“ [136].

Unglaubwürdig ist das soweit nicht, da es außer einem Computer mit Internetanschluss nichts braucht. Auf der anderen Seite ist nicht abzustreiten, dass die Syrian Electronic Army im Sinne der syrischen Regierung unter Assad arbeitet. Der syrische Präsident bedankte sich im Juni 2011 in einem Statement im Fernsehen bei der Syrian Electronic Army für ihre Aktivitäten [139]. Das war nur kurz nach der Gründung der Syrian Electronic Army im Mai 2011 [139].

Wie eingangs erwähnt war der Fall 2014 keine einmalige Aktion der Syrian Electronic Army, sondern nur ein ausgewählter Fall. [134] schreibt etwa 70 Angriffe auf verschiedene Ziele im Zeitraum zwischen Juni 2011 und Juni 2015 der Syrian Electronic Army zu. Insgesamt bietet [134] eine lange Liste mit allen Cyber-Angriffen, die in der Zeit des Bürgerkriegs in Syrien zwischen 2011 und 2016 stattfanden. Tabelle 12: Angriffe der Syrian Electronic Army [134] bietet einen Ausschnitt dieser Liste und beinhaltet die Angriffe, die der Syrian Electronic Army zugeschrieben wurden. Die Tabelle gliedert sich in Datum des Angriffs und dem betroffenen Ziel in doppelter Spaltenführung. Hauptsächlich wurden Angriffe auf Medienunternehmen gestartet, aber auch staatliche Einrichtungen und beispielsweise Universitäten zählten zu den Zielen der Syrian Electronic Army. Ziel von Tabelle 12 ist es nicht weiter Informationen über Fälle von Cyber-Terrorismus zu sammeln, welche dann schlussendlich verwertet werden, sondern dient nur zum Überblick der zahlreichen Angriffe der Syrian Electronic Army. Es wurde auch nicht näher auf die von [134] verwendeten Beschreibungen der Ziele eingegangen, um die Übersicht möglichst kurz zu halten. Der in dieser Arbeit aufgegriffene Fall ist ebenfalls in der Tabelle gelistet und kursiv gekennzeichnet. Tabelle 12 enthält zur besseren Lesbarkeit zum Teil deutsche Übersetzungen der originalen Begriffe, die von [134] verwendet wurden.

Datum	Ziel	Datum	Ziel
6. Juli 2011	Universität von Kalifornien	23. Juli 2013	Viber
24. Juli 2011	Anonymous	29. Juli 2013	USA
8. August 2011	Anonymous	7. August 2013	Channel 4
26. September 2011	Harvard Universität	14. August 2013	New York Post
29. Jänner 2012	Al-Jazeera	17. August 2013	CNN, Time, Washington Post
24. März 2012	Al-Arabiya	22. August 2013	Sharethis
24. April 2012	Al-Arabiya	28. August 2013	Twitter, New York Times, Huffington Post
26. April 2012	LinkedIn	3. September 2013	USA
17. Juli 2012	Anonymous	10. September 2013	FOX
3. August 2012	Reuters	30. September 2013	Global Post
5. August 2012	Reuters	19. Oktober 2013	Qatar
10. September 2012	Al-Jazeera	28. Oktober 2013	USA
5. Jänner 2013	MasterCard	8. November 2013	Vice
8. Jänner 2013	Saudi-Arabien	1. Dezember 2013	Time
3. Februar 2013	Haaretz	12. Dezember 2013	Matthew VanDyke
7. Februar 2013	Sky News Arabia	1. Jänner 2014	Skype
26. Februar 2013	AFP	11. Jänner 2014	Microsoft
1. März 2013	The Qatar Foundation	*15. Jänner 2014*	*Saudi-Arabien*
5. März 2013	France 24 Arabia	23. Jänner 2014	CNN
15. März 2013	Deutche Welle Arabic	1. Februar 2014	eBay
17. März 2013	Human Rights Watch	14. Februar 2014	Forbes
21. März 2013	BBC Arabic	19. Februar 2014	FC Barcelona
16. April 2013	NPR	17. März 2014	Syrian National Coalition
20. April 2013	CBS News	29. April 2014	RSA Konferenz
23. April 2013	AP	7. Mai 2014	Wall Street Journal
29. April 2013	The Guardian	23. Juni 2014	Reuters
6. Mai 2013	E! Online	28. Juni 2014	Israel
8. Mai 2013	The Onion	4. Juli 2014	Israel
20. Mai 2013	The Telegraph	2. Oktober 2014	Unicef
25. Mai 2013	ITV News	27. November 2014	The Independent, The Telegraph, CNBC, Canadian Broadcasting corp., Boston Globe
26. Mai 2013	SKY	17. Dezember 2014	International Business Times
5. Juni 2013	Türkei	20. Jänner 2015	Le Monde
17. Juni 2013	Truecellar	12. Februar 2015	Syrian Observatory
20. Juli 2013	Tango	31. März 2015	Web hosting services
20. Juli 2013	Reuters	14. Mai 2015	Washington Post
23. Juli 2013	DailyDot	8. Juni 2015	USA

Tabelle 12: Angriffe der Syrian Electronic Army [134]

Ziel

Beim Angriff auf Saudi-Arabien 2014 wurden insgesamt 17 Webseiten gehackt [94]. Die Angreiferinnen und Angreifer stellten die verunstalteten Webseiten auch auf www.zone-h.org, wo sie aber mittlerweile nicht mehr eingesehen werden können. Folgende arabische Webseiten waren betroffen:

- www.aldoriyah.gov.sa
- www.almajmah.gov.sa
- www.alhotah.gov.sa
- www.alduwadimi.gov.sa
- www.alquwayiyah.gov.sa
- www.alghat.gov.sa
- www.huraymila.gov.sa
- www.shaqra.gov.sa
- www.almuzahmiyah.gov.sa
- www.alhariq.gov.sa
- www.alsulayyl.gov.sa
- www.thadiq.gov.sa
- www.duruma.gov.sa
- www.rumah.gov.sa
- www.imara-mag.gov.sa
- www.alsolh.gov.sa
- www.riyadh.gov.sa

Angriff

Die Syrian Electronic Army nutzt für gewöhnlich Social Engineering [95], Phishing [95] [140] und Distributed Denial of Service Angriffe [140], um ihren Zielen Schaden zuzufügen.

Folgen

Obwohl die Veränderungen auf den Webseiten nicht mehr aus erster Hand einsehbar sind, ist aufgrund der Veröffentlichung der Seiten auf einem Portal für gehackte Webseiten davon auszugehen, dass die Angreiferinnen und Angreifer erfolgreich die Kontrolle über die betroffenen Seiten aus dem Abschnitt Ziel übernommen haben. Innerhalb kurzer Zeit wurden die betroffenen Webseiten offline genommen und waren nicht mehr erreichbar [95] [135]

3.7. Cyberangriffe auf Südkorea

Das Land Südkorea wurde am 20.März 2013 Opfer von einem Cyber-Angriff, welcher Schäden in mehreren Nachrichtenagenturen und Banken verursachte. Der Angriff ist auch unter dem Namen „DarkSeoul“ und „Operation Troy“ bekannt.
[92] [141]

Angreiferin/Angreifer
Aufgrund der gefundenen Spuren, wie beispielsweise der verwendeten Malware und der IP-Adresse der Angreiferin beziehungsweise des Angreifers, konnte man zunächst schnell Rückschlüsse darauf ziehen, wer vermutlich hinter den Angriffen steht. Beginnend bei der IP-Adresse ließ diese zunächst darauf schließen, dass der Hacker oder die Hackerin aus China stammt [141]. Eine IP-Adresse allein beweist an dieser Stelle allerdings noch eher wenig, da der Angriff seinen Ursprung vermutlich nicht an dieser Adresse hatte. Einem Bericht aus [142] zufolge nutzen allerdings meist nordkoreanische Hackerinnen und Hacker routinemäßig chinesische IP-Adressen, um ihre Angriffe zu verschleiern. Im Zuge der Aufklärungsarbeiten, welche von McAfee durchgeführt wurden, konnten die Spuren von zwei Gruppierungen gefunden werden. Bereits im Jahr 2011 wurde Südkorea Opfer von Cyber-Angriffen. Damals bekannte sich die „NewRomanic Cyber Army“ in einem Statement zu den Angriffen:

„Hi, Dear Friends, We are very happy to inform you the following news. We, NewRomanic Cyber Army Team, verified our #OPFuckKorea2003. We have now a great deal of personal information in our hands. Those includes; 2.49M […] member table data, cms_info more than 50M from […]. Much information from […]. We destroyed more than 0.18M of PCs. Many auth Hope you are lucky. 11th, 12th, 13th, 21st, 23rd and 27th HASTATI Detachment. Part of PRINCIPES Elements. p.s For more information, please visit www.dropbox.com login with joseph.r.ulatoski@ gmail.com::lqaz@WSX3edc$RFV. Please also visit pastebin.com.“ [143][17]

Beim Vergleich der damaligen Malware mit jener von 2013 konnten die Ermittler Hinweise darauf finden, dass die NewRomanic Cyber Army auch bei den Angriffen von 2013 mitverantwortlich ist. Im Folgenden sind die gefundenen Spuren, die die Rückschlüsse auf NewRomanic Cyber Army ermöglichten, aufgelistet:

- Jene Software, die zum Löschen der Master Boot Records verwendet wurde (siehe Abschnitt Angriff für weitere Informationen), enthielt die Strings „Principes“ und „Hastati“.
- In einer Pop-up Nachricht auf der Webseite von Nocut News Korea wurden ebenfalls die Begriffe „Principes“ und „Hastati“ verwendet.
- Der Trojaner, welcher den Angreiferinnen und Angreifern den Remote-Zugriff erlaubte, hatte im Build-Path die Referenz „Make Troy“, wobei „Troy“ eine Region im antiken Rom war.

Die Begriffe „Principes“ und „Hastati“ bezeichnen antike römische Militäreinheiten und stehen damit genauso wie „Troy“ in Verbindung mit dem antiken Rom und der NewRomanic Cyber Army.

Eine weitere Spur deutet darauf hin, dass die NewRomanic Cyber Army nicht allein gehandelt haben muss. Es gibt entsprechende Hinweise auf Aktivitäten des „Whois“-Teams, nämlich in einem Wiper, der etwas anders als jene der NewRomanic Cyber Army funktioniert. Einen weiteren Hinweis auf eine Mitarbeit von Whois bietet eine Seite, die vom Mobilfunkanbieter LG Uplus angezeigt wurde. Sie zeigte eine Meldung, dass sie vom Whois Team gehackt wurde. Eine Besonderheit an dieser möglichen Zusammenarbeit der NewRomanic Cyber Army und dem Whois Team ist, dass sie beide bis zu diesem Vorfall keine bekannte Verbindung hatten.
[93] [143]

[17] Der Firmennamen ist [143] bekannt, aber wurde nicht veröffentlicht.

Schließlich stellen sich hier noch ein paar Fragen, die es zu beantworten gilt, nämlich:

- Könnte diese Cyberspionagekampagne von Nordkorea ausgehen, einem Land, das mit Südkorea bereits längere Zeit im Konflikt steht?
- Gibt es Hinweise darauf, dass die NewRomanic Cyber Army und das Whois-Team aus Nordkorea stammen oder von der Regierung Nordkoreas beauftragt wurden?

Im Jahr 2009, als diese Kampagne ihren vermeintlichen Ursprung hatte und man erstmals versuchte zu ergründen, wo die Angriffe ihren Ursprung haben, verdächtigte man die nordkoreanische Gruppe „Lab 110“. Berichten zufolge konnte der südkoreanische Geheimdienst (National Intelligence Service) an Informationen gelangen, wodurch sie darauf schließen können, dass der Angriff von Nordkoreas Verteidigungsministerium an Lab 110 befohlen wurde. Allerdings wurde dies auf Anfrage von verschiedenen Nachrichtenagenturen nicht nochmal bestätigt.
[144]

Ein weiteres Indiz auf einen Einfluss von Nordkorea sind die Zeitpunkte und das Ausmaß der Angriffe. So wurden beispielsweise im Zuge von Jahrestagen anlässlich des Koreanischen Krieges Angriffe gestartet [93]. Weitere Angriffe gab es als Folge von (Cyber-)Angriffen auf Nordkorea, für die Nordkorea Südkorea beschuldigt [141] [143].

Ziel
Der Angriff richtete sich nicht an ein einzelnes Ziel, sondern an einige Unternehmen, die in Südkorea angesiedelt sind und hauptsächlich in Südkorea geschäftstätig sind. Von den Angriffen betroffen waren hauptsächlich die eingangs erwähnten drei Banken und drei Nachrichtenagenturen:

- Shinhan Bank
- Nonghyup Bank
- Jeju Bank
- Korean Broadcasting System
- Munhwa Broadcasting Corporation
- Yonhap Television News
- LG Uplus (Mobilfunkanbieter)

[92] [93] [145]

McAfee vermutet hinter den Angriffen eine weitläufige Cyberspionagekampagne, genannt Operation Troy, welche bereits im Jahr 2009 ihren Ursprung hatte. Diese Kampagne zielt laut McAfee darauf ab, geheime Informationen über die militärischen Streitkräfte des Landes Südkorea zu extrahieren.
[143]

Angriff
Das Aufklärungsteam von McAfee konnte die wahrscheinliche Vorgehensweise der Angreiferinnen und Angreifer rekonstruieren und die nötigen Schritte beschreiben, welche zu den Ausfällen am 20. März 2013 führten. Die aufgelisteten Schritte beziehen sich auf die Ausfälle in den drei Banken und den drei Nachrichtenagenturen:

1. Der Trojaner für den Remote-Zugriff wurde am 26. Januar 2013 kompiliert.
2. Jene Komponente, die den Master Boot Record zahlreicher Systeme löschte, wurde am 31. Januar kompiliert.
3. Der Trojaner für den Remote-Zugriffe wurde als Phishing-Mail an ein Opfer innerhalb der Organisation geschickt. Dies geschah sehr wahrscheinlich bereits vor dem 20.März, möglicherweise können es sogar mehrere Wochen davor gewesen sein. Es wäre unrealistisch, dass mehr als 30 000 Benutzerinnen und

Benutzer an einem Tag von Spear Phishing betroffen sind. Mithilfe des Remote-Zugriffs konnten die Angreiferinnen und Angreifer einen internen Server der Nonghyup Bank übernehmen [142], welcher üblicherweise Updates an Clients verteilt. Durch Übernahme dieses Servers konnten die Angreiferinnen und Angreifer den Trojaner zum Löschen der Master Boot Records verteilen.

4. Der Dropper-Trojaner, welcher dafür sorgte, dass die Wiper für den Master Boot Record installiert werden, wurde am 20. März nur wenige Stunden vor dem Angriff, kompiliert.
5. Schließlich wurde dieser Dropper-Trojaner auf die Systeme der betroffenen Organisationen verteilt und die Master Boot Records wurden gelöscht.

[143]

Die beim Angriff beteiligten Komponenten aus dem Angriffshergang sind für eine bessere Übersicht in Tabelle 13: Verwendete Komponenten für den Angriff auf Südkorea [143] aufgelistet.

Komponente	Zweck	Dateigröße	Kompilierungsdatum
Dropper-Trojaner	Installiert den Master Boot Record Wiper.	418KB	20.März 2013
Master Boot Record Wiper	Löscht den Master Boot Record der Festplatten.	24KB	31.Januar 2013
Trojaner für Remote-Zugriff	Ermöglicht den Angreifern einen Remote-Zugriff auf die betroffenen Systeme.	46KB	26.Januar 2013

Tabelle 13: Verwendete Komponenten für den Angriff auf Südkorea [143]

Folgen

In den betroffenen Firmen wurden die Master Boot Records gelöscht, weshalb diese Systeme nicht mehr ordnungsgemäß funktionierten. Die Schäden betrafen vor allem die Banken, wo schließlich Geldausgabeautomaten und Online-Banking nicht mehr funktionierten. Allerdings konnten die Firmen bereits am nächsten Tag die ausgefallenen Systeme wiederherstellen. Insgesamt waren von den Systemlöschungen etwa 32 000 Computer betroffen. Außerdem sind die großen Datenverluste vor allem aus dem Jahr 2011 nicht zu vergessen. Ob die Hackerinnen und Hacker sie wirklich gelöscht haben oder im Zuge der Angriffe 2009 und 2013 noch weitere Informationen erbeuten konnten, ist schwer feststellbar.
[141]

3.8. Ukrainische Stromversorger

Am 23. Dezember 2015 gab es in der Ukraine Stromausfälle, welche durch einen Cyber-Angriff auf einige Stromversorger ausgelöst wurden. Dabei waren mehrere Regionen in der Ukraine betroffen. Während der Wiederherstellungszeit funktionierte die Stromversorgung nur eingeschränkt, worunter etwa 225 000 Kundinnen und Kunden litten. Dennoch konnte man die Stromversorgung sehr schnell wiederherstellen. Die Ausfälle dauerten nur zwischen einer bis sechs Stunden [146].
[96] [97] [147]

Angreiferin/Angreifer
Bei dem Angriff auf die Infrastruktur wurden Spuren der Malware BlackEnergy (BE) und KillDisk gefunden [148] [149]. Weitere Informationen zu der Malware selbst folgen im Abschnitt Angriff. Insbesondere BlackEnergy wird einer russischen Gruppierung zugewiesen, welche unter den Namen „Sandworm“ [149] bekannt ist. Aufgrund von Ähnlichkeiten geht man davon aus, dass die Gruppe auch als „Quedagh“ [150] und „Voodoo Bear“ [151] operiert beziehungsweise bekannt ist. Eine dieser Ähnlichkeiten sind Referenzen zu dem Roman „Dune“ von Frank Herbert [152], welche sich in der Malware wiederfinden [151] und auch zum Namen der Gruppe Sandworm führen [149]. Bis zum Zeitpunkt der Angriffe auf die Ukraine war die Gruppierung eher für Datendiebstahl bekannt, der verursachte Blackout ist für die Gruppierung neu [153]. Seit wann genau die Gruppe aktiv ist, ist schwer zu sagen, da sich hier immer wieder unterschiedliche Referenzen finden. Die Malware BlackEnergy geht laut [153] und [154] bis ins Jahr 2007 zurück. Im Gegensatz dazu sieht [155] die Ursprünge der Organisation etwa im Jahr 2009. Geht man nach den anderen Namen Voodoo Bear oder Quedagh so finden sich hier für Voodoo Bear etwa Ursprünge im seit zumindest 2011 [151] und für Quedagh aufgrund der Verwendung von BlackEnergy wieder Wurzeln im Jahr 2007 [150].

In einer Sache ist man sich allerdings einig, nämlich, dass es sich bei Sandworm um eine Gruppierung aus Russland handelt. Der ukrainische Energieminister gab in einem Interview [156] an, dass die Angriffe über einen russischen Internetdienstanbieter stattfanden und auch die Telefonanrufe aus Russland kamen (Anmerkung: Es wurde versucht den Telefonsupport der Stromdienstanbieter zu sabotieren, damit diese möglichst lange nichts vom Angriff mitbekommen und spät reagieren. Für weitere Details siehe Abschnitt Angriff). Ebenso überzeugt von den Spuren nach Russland sind Analystinnen und Analysten der Schäden [157]. Außerdem verlief der Angriff zugunsten staatlicher Interessen der russischen Regierung [151]. Weiters sieht man den Angriff unter anderem als eine Reaktion im Konflikt zwischen Russland und der Ukraine, welcher seit der Annexion der Krim durch Russland im Jahr 2014 herrscht, da diese Annexion von ukrainischer Seite negativ aufgenommen wurde [156] [157].

Ziel
Hauptziel des Angriffs waren drei Stromversorger (oftmals auch als „Oblenergos“ bezeichnet) in den drei ukrainischen Regionen „Prykarpattia“, „Chernivtsi“ und „Kyiv“ [97]. Im Folgenden werden die Stromversorger in den Regionen auch als „Prykarpattiaoblenergo“, „Chernivtsioblenergo“ und „Kyivoblenergo“ bezeichnet und spiegeln somit Region und Stromversorger wider. Die genannten drei betroffenen Regionen der Ukraine sind in Abbildung 10: Betroffene Regionen der ukrainischen Stromausfälle [158] ersichtlich. Prykarpattia und Chernivtsi sind im Westen des Landes angesiedelt, während sich die Region der Hauptstadt Kyiv zentral im Norden befindet.

Abbildung 10: Betroffene Regionen der ukrainischen Stromausfälle [158][18]

Neben diesen drei Zielen wurden Spuren der Malware BlackEnergy und KillDisk auch bei zwei anderen ukrainischen Unternehmen gefunden, die auf einen Zusammenhang deuten. Es handelt sich dabei um eine Bergbaufirma und einen Eisenbahnbetreiber. Bei der Bergbaufirma wurden die Hashwerte von manipulierten Dateien miteinander verglichen und dabei Ähnlichkeiten gefunden beziehungsweise Spuren, die ebenfalls auf BlackEnergy und KillDisk hinweisen. Gleiches gilt für IP-Adressen, mit denen die Schadsoftware kommuniziert hat. Bei den gefundenen Spuren geht man von einem Verwendungszweck zwischen November und Dezember 2015 aus. Das heißt die Malware war bei diesem Unternehmen bereits vor den Vorfällen bei den Stromversorgern aktiv. Beim Eisenbahnunternehmen konnten nur Spuren von KillDisk gefunden werden, allerdings ist nicht auszuschließen, dass BlackEnergy auch hier aktiv war. Insgesamt sind bei den Angriffen auf die Energieversorger, dem Bergbauunternehmen und dem Eisenbahnbetreiber Ähnlichkeiten zu verwendeter Malware, Infrastruktur, Namensgebung und eingesetztem Zeitraum zu beobachten. Daraus lassen sich drei mögliche Szenarien ableiten, wie die Angriffe zusammenhängen:

- Man wollte die ukrainische Stromversorgung, das ukrainische Transportsystem und den ukrainischen Bergbau lahmlegen, um das ganze Land zu destabilisieren.
- Es wurde versucht Malware auf mehreren kritischen Infrastrukturen zu installieren und dann jene zu übernehmen, wo es am einfachsten ist.
- Das Bergbauunternehmen und der Eisenbahnbetreiber dienten nur zu Testzwecken und die Stromversorger waren das eigentliche Ziel.

[159]

Insgesamt spricht auch [160] von sechs Zielen, bei denen ein Angriff versucht wurde. Unter den Zielen liegen primär die drei betroffenen Stromversorger. Allerdings hält man sich mit Namen betroffener Organisationen in

[18] Aus dem originalen Bild von [158] wurde die Region der Krim entfernt, da sie bereits zur Zeit des Angriffs kein Teil der Ukraine mehr war.

[160] bedeckt, es wird nur angegeben, dass sie alle Betreiber kritischer Infrastrukturen sind. Es ist aber anzunehmen, dass es sich zumindest bei zwei der drei zusätzlichen Ziele um jene aus [159] handelt.

Angriff

Die Auswirkungen der Angriffe waren am 23. Dezember 2015 erstmals zwischen etwa 15:30 und 16:30 nach lokaler Ortszeit spürbar [148]. Ursache dafür war die Aktivierung der Leitungsschutzschalter, welche normalerweise dazu dienen den Strom aus Sicherheitsgründen abzuschalten [158]. Diese wurden allerdings nicht aus diesem Grund aktiviert, sondern von Hackerinnen und Hackern dazu missbraucht Schaden anzurichten [158]. Einen guten Überblick über die vermeintliche Vorgehensweise der Angreiferinnen und Angreifer bieten die Autoren aus [158], welche die nötigen Schritte in acht Phasen zusammengefasst haben. Für einen besseren Überblick findet sich der gesamte Tathergang auch in Abbildung 11: Angriffshergang auf Stromversorger [158]:

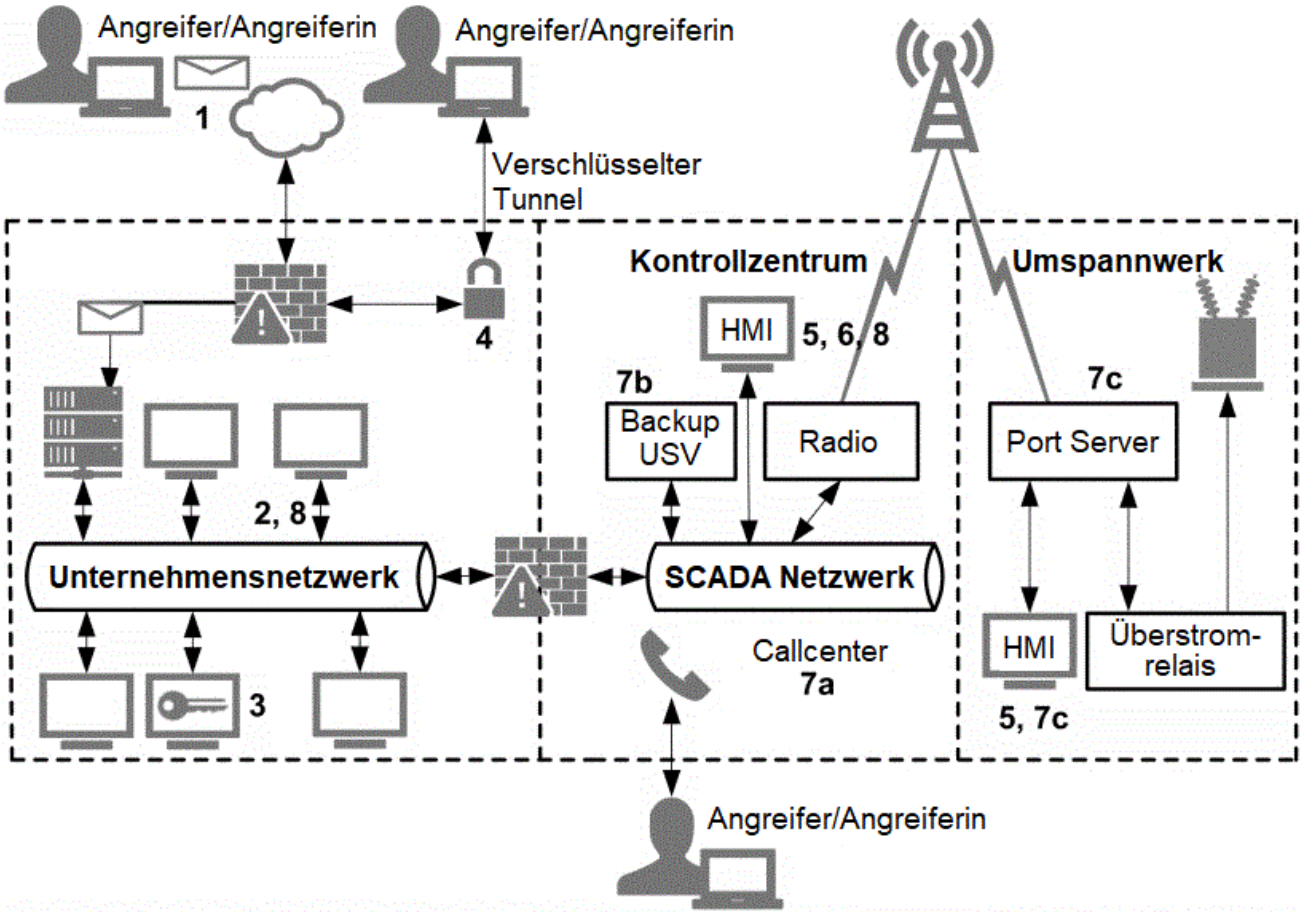


Abbildung 11: Angriffshergang auf Stromversorger [158]

1. Die Angreiferinnen und Angreifer begannen zunächst damit ihre Malware BlackEnergy in Version 3 (BE3) mithilfe gezielter Phishing E-Mails an ihre Opfer auszuliefern [161]. Der E-Mail war ein manipuliertes Microsoft Office Dokument beigelegt, das ein Makro enthielt, welches die Installation von Malware, wie BlackEnergy, auf den Computern der Unternehmen durchführte [162].
2. Die installierten Tools inklusive BlackEnergy scannen das Netzwerk der Stromanbieter und zeigen den Angreiferinnen und Angreifern mögliche Wege in die Firmennetzwerke [163]. BlackEnergy konnte einige Computer in den Netzwerken der Stromanbieter kompromittieren. Allerdings ist nicht bestätigt, dass die Malware in die eigentlichen Angriffe involviert ist. Im April 2015 wurde zusätzliche Malware auf den

bereits infizierten Systemen installiert, was den Angreiferinnen und Angreifern einen einfacheren Zugang auf diese Computer gewährte [158].

3. Durch den Scan der Netzwerkinfrastruktur finden die Hackerinnen und Hacker den Microsoft Active Directory Server des Stromversorgers Prykarpattiaoblenergo und können mithilfe von Brute Force User Accountnamen und -passwörter von Benutzerinnen und Benutzern der Firma auslesen. In der Region Kyiv wurden die Passwörter mit einer unbekannten Methode ausgelesen. [160]
4. Mithilfe der gestohlenen Anmeldedaten können die Angreiferinnen und Angreifer eine verschlüsselte Virtual Private Network (VPN) Verbindung einrichten und auf die Human-Machine Interfaces (HMIs) zugreifen. Dabei verwendeten sie Tools wie beispielsweise Remote Desktop Protocol (RDP), Remote Administrator (Radmin) und Secure Shell (SSH).
5. Die Angreiferinnen und Angreifer scannen das Netzwerk und können schließlich auf die HMIs von 17 Stromverteilerzentren und das verbundene SCADA-Netzwerk (Supervisory Control and Data Acquisition) zugreifen. Diese Netzwerke sind zwar vom eigentlichen Unternehmensnetzwerk getrennt, allerdings waren die Firewall Regeln schlecht konfiguriert und erlaubten daher den Zugriff auf diese Systeme. Die HMIs sind mit 50 Umspannwerken verbunden.
6. Nun findet der eigentliche Angriff statt, indem die Hackerinnen und Hacker die Leitungsschutzschalter über das HMI dazu missbrauchen die Stromzufuhr abzuschalten. In diesem Moment ist es aber schon zu spät und die verantwortlichen Personen können die Aktionen der Hackerinnen und Hacker nur noch auf ihren Bildschirmen beobachten, aber selbst nicht mehr eingreifen, da ihre Passwörter geändert wurden und sie mit den Systemen nicht mehr interagieren können [161]. Die Leitungsschutzschalter wurden nacheinander abgeschalten und auch die Mauscursorbewegungen, die von den ukrainischen Mitarbeiterinnen und Mitarbeitern beobachtet werden konnten, ähnelten einer Person und nicht einer Maschine, was für einen koordinierten Angriff mehrerer Beteiligter spricht [158] [161]. Schließlich gelang es den Stromversorgern aber das SCADA System und die VPN-Verbindungen abzuschalten [158] und im manuellen Betrieb der Leitungsschutzschalter die Stromversorgung wiederherzustellen [164].
7. Zusätzlich zu den eigentlichen Angriffen versuchen die Hackerinnen und Hacker die Wiederherstellung der Systeme so lange wie möglich zu verhindern. Dazu führen sie einige weitere Aktionen aus.
    a. Mithilfe zahlreicher Anrufe im Callcenter der Stromversorger Prykarpattiaoblenergo und Kyivoblenergo bewirken die Angreiferinnen und Angreifer einen Denial of Service der Telefonie (Telephony Denial of Service - TDoS), was dazu führt, das legitime Anrufe, die den Ausfall melden möchten, nicht durchgestellt werden können. [158]
    b. Die Unterbrechungsfreie Stromversorgung (USV) gerät ebenfalls ins Visier der Angreiferinnen und Angreifer und sie schalten sie ab. Diese USV dient dazu die Systeme der Stromversorger mit Strom zu versorgen und zögerte damit die Wiederherstellungszeit hinaus. [161]
    c. Die Firmware einiger Serial-to-Ethernet Konverter in den Umspannwerken wird korrumpiert, damit diese nicht mehr funktionieren [163].
8. Abschließend wurden mithilfe von KillDisk die Spuren gelöscht. KillDisk löscht viele Dateien auf den Zielsystemen und beschädigt den Master Boot Record, sodass die betroffenen Systeme nicht mehr funktionieren. [160]

Die von den Angreiferinnen und Angreifern eingesetzte Malware BlackEnergy 3 ist eine Weiterentwicklung der BlackEnergy Malware, welche seit 2007 eingesetzt wird [154]. Eine Übersicht über BlackEnergy und die integrierten Features und Weiterentwicklungen seit 2007 bis zum Einsatz 2015 gegen die Ukrainie findet sich in Tabelle 14: BlackEnergy Malware Entwicklung [154]. Tabelle 14 enthält die Versionen BlackEnergy 1 (BE1), BlackEnergy 2 (BE2), BlackEnergy Lite (Lite) und BlackEnergy 3 (BE3), wobei die Abkürzungen in Klammern nur für Tabelle 14 gelten. Vorhandene Features sind mit einem „X“ gekennzeichnet. Aufgrund der Weiterentwicklung und der Geschichte von BlackEnergy sind Features enthalten, welche im Laufe der Zeit hinzugefügt wurden, um die damaligen Zielsysteme anzugreifen. Das heißt nicht jedes Feature muss unbedingt beim Angriff auf die ukrainischen Stromversorger im Einsatz gewesen sein, wenn es in der Liste ist.

Feature	BE1	BE2	BE Lite	BE 3
GUI Build Tools	X	X	X	X
Plugin Support		X	X	X
Denial of service	X	X	X	X
Command & Control Server	X	X	X	X
Anti-Virus Obfuscation	X	X	X	X
Kernel rootkit			X	X
x64 support			X	X
bypass driver signing				X
Reside only in memory				X
rundll			X	X
Detection of virtual environment				X
Anti-debugging methods				X
Detect security countermeasures				X

Tabelle 14: BlackEnergy Malware Entwicklung [154]

Folgen

Die größten Auswirkungen hatte der Vorfall, wie eingangs erwähnt, auf private Haushalte, konkret etwa 255 000 Personen, die für eine bis sechs Stunden ohne Strom waren [96]. Etwa 80 000 davon stammen aus der Region Ivano Frankivisk, welche von Prykarpattiaoblenergo versorgt werden [153]. Insgesamt entsprechen die 225 000 Betroffenen etwa 1% aller Kundinnen und Kunden der Stromversorger [147]. Das klingt vielleicht wenig, wenn man die Gesamtanzahl der ukrainischen Bevölkerung von 2015 mit 42,59 Millionen bedenkt [165]. Trotzdem waren 103 Städte komplett im Dunklen und weitere 186 teilweise ohne Strom [157].

Auch bei den Stromversorgern selbst gab es Schäden. Durch die Korrumpierung der Firmware in den Umspannwerken funktionierten diese nicht mehr. Allein bei Prykarpattiaoblenergo waren es 27 Umspannwerke.

3.9. Gestoppter Cyberangriff auf Israel

Am 4.Mai 2019 stoppte das israelische Militär einen Cyberangriff der Terrorgruppe Hamas. Es ist nicht bekannt, was genau das Ziel der terroristischen Hackerinnen und Hacker von Hamas war. Israel gibt dazu keine Informationen preis, da sie ansonsten fürchten Hamas könnte diese Informationen zu ihrem Vorteil nutzen. Das Besondere an diesem Fall ist die Art und Weise, wie die Israel Defense Forces den Angriff von Hamas verhindert haben. Anstatt den Angriff der Terroristinnen und Terroristen mit technischen Mitteln, das heißt im Cyber-Bereich, zu verhindern, wurde mit einem Luftangriff auf das Gebäude, von dem der Angriff ausging, reagiert.
[98] [166]

Angreiferin/Angreifer
Die sowohl von der Europäischen Union [7], als auch von den Vereinigten Staaten [8], als terroristisch eingestufte Organisation Hamas versuchte einen Cyber-Angriff auf Israel. Hamas selbst ist eine muslimische Vereinigung, welche seit 1987 besteht. das Wort Hamas ist arabisch (original „حماس“ geschrieben) und bedeutet in etwa „Begeisterung“ beziehungsweise „Eifer“. In der von Hamas 1988 veröffentlichten Charta gibt Hamas an, dass Palästina eine islamische Heimat ist, die nicht von Andersgläubigen bewohnt und verwaltet werden darf. Ferner hat jede palästinensische Muslimin und jeder palästinensische Muslim die Pflicht in einem Heiligen Krieg die Kontrolle über Palästina zurückzuerlangen. Der Angriff von Hamas ging von Gaza, der größten Stadt im Gazastreifen, aus. Der Gazastreifen wird seit 2007 von Hamas kontrolliert. Der Konflikt zwischen Israel und Hamas ist nicht neu, bereits seit mehreren Jahren finden hier immer wieder militärische Konflikte statt.
[167]

Ziel
Der Kommandant der Cyber Division der Israel Defense Forces, genannt Dalet, (Der Name des Kommandanten ist unbekannt. Er ist nur unter dem Pseudonym Brigadier General „Dalet“ öffentlich bekannt, wobei Dalet neben seinem militärischen Rang den ersten hebräischen Buchstaben seines Namens darstellt [98]) spricht davon, dass es sich bei den Cyberangriffen vom 4. Mai 2019 um Angriffe handelt, die darauf ausgerichtet waren die Lebensqualität der israelischen Bürgerinnen und Bürger zu beeinträchtigen [168]. Warum Dalet keine weiteren Informationen liefert begründet [168] beispielsweise damit, dass es keinen Grund dafür gibt, anzugeben wo Hamas erfolgreich oder fast erfolgreich war. Ziele gibt es in Israel genug, die ins Visier von Hamas geraten sein könnten [168]. Basierend auf der Aussage von Dalet, die Angriffe waren darauf ausgerichtet die Lebensqualität der israelischen Bürgerinnen und Bürger zu beeinträchtigen, liefert [168] ein paar Ideen für mögliche Ziele. [168] spricht von kritischer ziviler Infrastruktur, von der Unterbrechung sicherer Kommunikationen und der Einmischung in laufende militärische Operationen, welche in Diebstahl und Spionage resultieren.

Angriff
Israel selbst gibt keine Informationen darüber preis, was angegriffen werden sollte beziehungsweise vermutlich in Ansätzen angegriffen wurde. Allerdings muss man von israelischer Seite einen Cyber-Angriff in gewisser Weise beobachten haben, da man Gegenmaßnahmen einleitete. Trotzdem fehlen Details zu den Angriffen und daher gibt es auch keine Informationen über die Art und Weise des Angriffs. Eine Information der Cyber Division der Israel Defense Forces lautet, dass es sich um keinen sehr fortschrittlichen Angriff handelte und man den Angreiferinnen und Angreifern immer einen Schritt voraus gewesen sei [98]. Durch Veröffentlichung genauerer Informationen würde Hamas aber wissen welche Angriffe von Israel mitverfolgt werden konnten. Es ist nicht auszuschließen, dass Hamas erfolgreich einen Zugang auf Systemen in Israel etablieren konnte. Wenn Israel nun veröffentlicht bei welchen Systemen sie Angriffe von Hamas erkannt haben, dann besteht einerseits die Gefahr etwas zu viel Information preiszugeben, indem beispielsweise das betroffene System beschreiben wird, was Hamas einen Vorteil für den nächsten Angriff gibt. Andererseits erfährt Hamas, dass unter Umständen ein Angriff nicht erkannt wurde, wenn Israel alle bekannten Angriffsziele offenlegt. Dadurch kann Hamas versuchen auf den unerkannten vorhandenen Zugriffsmöglichkeiten beim nächsten Cyber-Angriff aufzubauen. Die Israel Defense Forces sprechen von keinen sehr fortschrittlichen Angriffen, was darauf zurückgeführt werden kann, dass es sich bei diesen Angriffen nur um Ablenkungsmanöver handelte, die von einem größeren bis jetzt

unentdeckten Angriff ablenken sollten. Dieser Angriff könnte aber unentdeckt geblieben sein, da Hamas nicht mit einem derartigen Vergeltungsschlag gerechnet hatte und dadurch auch diesen eigentlichen Angriff nicht durchführen konnte. Eine letzte Theorie wirft [168] auf, dass Hamas durchaus erfolgreich bei seinen Angriffen gewesen sein kann und Israel dies nicht bestätigen will.

Trotzdem ist es an dieser Stelle schwer nachzuvollziehen wie gut Hamas im Bereich Cyber-Terrorismus wirklich aufgestellt war und welche Strategien die beiden Seiten nun verfolgen, da jede veröffentlichte Information dem Kontrahenten behilflich sein kann. Die Entscheidung diesen Cyber-Angriff mit militärischer Gewalt zu vergelten scheint nicht aus einer Kurzschlussreaktion heraus entstanden zu sein, da man sich von israelischer Seite nicht anders zu wehren wusste, sondern war eine gemeinsame Aktion von Einheit 8200, (dem militärischen Nachrichten und Aufklärungsdienst der Israel Defense Forces) der Teleprocessing Abteilung der Israel Defense Forces und dem israelischen Geheimdienst Shin Bet [168].

Folgen
Auch wenn der Angriff von Hamas auf Israel laut Angaben der Israel Defense Forces keine Schäden für Israel verursacht hat, gibt es andere Folgen und Konsequenzen [98]. Zunächst hatte der Angriff Folgen für die Angreifer selbst. Israelische Kampfflugzeuge griffen das Gebäude, von dem aus der Cyber-Angriff stattfand, an und zerstörten es [166] [169]. Die Israel Defense Forces sprachen an dieser Stelle via Twitter von einer erfolgreichen „cyber defense operation“ [169], man hatte „HamasCyberHQ.exe“ [169] entfernt.

An dieser Stelle wurde ein Cyber Angriff beinahe unmittelbar durch einen militärischen Angriff gestoppt. Eine ähnliche Situation ist auf den ersten Blick bis jetzt noch nicht eingetreten, was zu neuen Fragen führt. Einige dieser Fragen kommen beispielsweise von [166]:

- „When a nation suffers a cyberattack, should it retaliate only through cyberattacks, or should it feel free to use physical force?” [166].
- „Is moving from cyberattacks to physical attacks an escalation, which might cause further retaliation?“ [166]
- „And if a nation moved in the opposite direction - responding to a physical attack with a cyberattack - should that be seen as a dangerous escalation?“ [166][19]

Der Autor aus [168] folgert in seinem Artikel, dass dies im Grunde Hackerinnen und Hacker mit anderen militärischen Zielen, wie Kommandozentralen, Flugplätzen und Treibstoffdepots gleichsetzt. Bis zu diesem Zeitpunkt war das der zweite Fall, in welchem man mit einem militärischen Schlag gegen Cyber-Terrorismus vorging. Bereits 2015 wurde Junaid Hussain von einer Dohne der Vereinigten Staaten getötet. Dieser Anschlag wurde allerdings lange vorher geplant und betraf nur eine einzelne Person.
[166] [168]

Dennoch darf man bei dieser Kritik an der militärischen Vergeltung dieses Angriffs den Kontext der Ereignisse nicht außer Acht lassen. Am betroffenen Wochenende im Mai 2019 wurden laut der Israel Defense Forces etwa vier Israelis von mehr als 600 Raketen aus Gaza getötet [170]. Die Cyber-Angriffe der Hamas passierten in diesem Zeitraum und waren Teil der umfassenden Angriffe. Eine Hypothese, aufgestellt von [166], besagt, dass Israel die Kriegssituation nur ausgenutzt hat, um die Cyber-Kapazitäten von Hamas kostengünstig und mit geringem Risiko auszuschalten.

[19] Zu Deutsch:

- Wenn eine Nation von einem Cyberangriff betroffen ist, sollte sie dann nur durch Cyberangriffe zurückschlagen oder sich frei fühlen physische Gewalt anzuwenden?
- Ist der Wechsel von Cyberangriffen zu physischen Angriffen eine Eskalation, die zu weiteren Vergeltungen führen könnte?
- Und wenn sich eine Nation in die entgegengesetzte Richtung bewegt - als Reaktion auf einen physischen Angriff mit einem Cyberangriff - sollte das als gefährliche Eskalation angesehen werden?

4. Zusammenfassung der Fälle

Für eine bessere Übersicht der Fälle von Cyber-Terrorismus, die in Kapitel 3 Fälle von Cyber-Terrorismus vorgestellt wurden, dient dieses Kapitel als Zusammenfassung der wichtigsten Informationen zu den Fällen. Zusätzlich soll ein Überblick über alle behandelten Fälle entstehen, welcher anders als in Kapitel 3 die Fälle nicht mehr für sich getrennt voneinander betrachtet, sondern miteinander vergleicht. Die Zusammenfassung erfolgt auf Basis der vier behandelten Abschnitte aus Kapitel 3, nämlich Angreiferin/Angreifer, Ziel, Angriff und Folgen. Der dadurch entstehende Gesamtüberblick wird anschließend in Kapitel 5. Prävention von Cyber-Terrorismus herangezogen, um Maßnahmen zur Vermeidung abzuleiten und bestehende Maßnahmen aus früheren Arbeiten wie jenen von [64] und [77] zu bewerten. Außerdem soll untersucht werden, ob bereits existierende Frameworks zur Beschreibung von Cyber-Bedrohungen dazu genutzt werden können, in Zukunft einen besseren Überblick über Fälle von Cyber-Terrorismus zu bieten.

4.1. Angreiferin/Angreifer

Nicht in jedem der behandelten Fälle ist es klar, wer hinter den Angriffen steht. Bei anderen Fällen ist es stattdessen mit vielen Beweisen und Statements relativ eindeutig festzustellen. Beginnend bei Fall Nummer 1, welchem die Gruppe der „Liberation Tigers of Tamil Eelam“ als Angreifer zugeordnet wurde, kann man zumindest das zurückgelassene Statement, in welchem sich die Gruppe bekannte und ihren Beweggrund angab, dafür auslegen, dass sie es tatsächlich waren. Weiters gibt es wenige Anzeichen für andere Täter oder Gegenargumente. Gleiches gilt auch für den 2. Fall um den Aum Shinrikyo Kult. Nachdem die Daten hier bei den Tätern gefunden wurden und auch die Beweggründe sehr gut nachvollziehbar sind, ergibt sich ein ziemlich klares Bild. In Fall 3 zu Estland ist das zwar nicht ganz so sicher, aber trotzdem ist es immer noch die plausibelste Erklärung, dass die Kreml-Jugend den Angriff koordinierte und als Drahtzieher fungierte. Die einzige Ausnahme ist der verurteilte Angreifer Dmitri Galuškevitš, welcher tatsächlich identifiziert wurde. Ähnliches gilt für Fall 4 in Georgien. Ein Gesicht zu dem Fall, wie bei Estland, gibt es allerdings nicht. Trotzdem kann man zumindest mit überwiegender Wahrscheinlichkeit davon ausgehen, dass Russland in die Geschehnisse involviert ist.

So gut wie keine Informationen zum Angreifer gibt es zu Fall 5 in den Vereinigten Staaten. Allerdings blieben hier großartige Folgen und Angriffe aus und man kämpfte eher gegen eine Spionagekampagne. Bei Fall 6, welcher sich um die Syrian Electronic Army dreht, sprechen sowohl die Beweise als auch die Bekennung der Gruppe selbst wieder ganz klar dafür, dass die Syrian Electronic Army wirklich der Täter ist. Klare Statements gibt es in Fall 7 in Südkorea zwar nicht, dafür aber eine Aufarbeitung des Falls, welche Spuren zu zwei bekannten Hacker-Gruppen gefunden hat. Dass die Operationen von Nordkorea ausgehen ist ebenfalls nicht auszuschließen. Bei der Analyse der Angriffe auf die Ukraine in Fall 8 gibt es wieder Spuren, die nach Russland führen und dort die Gruppe Sandworm verantwortlich machen. In Fall 9 zu Hamas und den Israel Defense Forces gibt es nur einseitige Informationen von Israel, dass sie angegriffen wurden. Aufgrund der kriegerischen Auseinandersetzung zwischen Hamas und Israel ist es zwar nachvollziehbar, dass ein Angriff von Seiten der Hamas stattfand, aber Beweise von einer dritten Partei gibt es nicht. Geht man davon aus, dass es einen Angriff gegeben hat, bleibt Hamas aufgrund des Konflikts mit Israel immer noch der wahrscheinlichste Angreifer.

Basierend auf den Fakten der verwendeten Quellen sind vier der Täterinnen und Täter mit überwiegender Wahrscheinlichkeit tatsächlich für die Angriffe verantwortlich. Hierfür wurden die Fälle 1, 2, 6 und 9 gewertet. In vier weiteren Fällen ist es zumindest ungefähr zu erahnen wer verantwortlich ist. Dazu zählen die Fälle 3, 4, 7 und 8. Beinahe gar keine Informationen gibt es nur in Fall 5 in den Vereinigten Staaten, Mitunter liegt dies aber an der Verschwiegenheit der Behörden dort. Dass es überhaupt Probleme mit Hackerinnen oder Hackern im Stromnetz gibt wurde 2009 bekannt, auch erst Jahre nachdem man intern die Probleme entdeckte.

Vier der Täter sind also mit ziemlicher Sicherheit für die Angriffe tatsächlich verantwortlich. Prinzipiell bedeutet das, in der Stichprobe an Fällen für Cyber-Terrorismus ist nicht einmal die Hälfte an Täterinnen und Tätern klar. Hinzu kommt allerdings, dass im Zuge von Aufklärungsarbeiten keine einzige Täterin beziehungsweise kein einziger Täter so gut identifiziert werden konnte, um mit Sicherheit auf sie oder ihn zeigen zu können. Bei den Fällen 1 und 6 bekannten sich die Täter selbst zu den Angriffen. Großartige Aufklärungen sind daher nicht nötig, wenn die Beweggründe nachvollziehbar sind und die Täterin oder der Täter plausibel erscheint. Fall 2 wurde eher durch Zufall entdeckt und gleichzeitig gelöst. In Fall 9 beschuldigte Israel sofort Hamas für die Angriffe und

behauptete nach der Zerstörung des Cyber-Zentrums, die Angriffe auf ihre Systeme hätten aufgehört. Die anfängliche Beschuldigung erfolgte aber nicht durch ein Expertenteam, welches zum Beispiel in einer längeren Aufklärungskampagne versuchte den Angriff zurückzuverfolgen und Hamas als Täter feststellen konnte. Vielmehr wurde schnell gehandelt und dabei der richtige Angreifer erwischt. Dies soll nicht bedeuten, dass die Identifikation des Angreifers in Fall 9 auf reinem Zufall basierte, sondern nur, dass man erst nach dem Gegenschlag sicher wusste, dass Hamas der Angreifer war.

Streng genommen kommt man zu dem Schluss, eigentlich keine einzige Täterin beziehungsweise keinen einzigen Täter allein durch das Aufarbeiten des Falls eindeutig identifizieren zu können. Einzige Ausnahme ist hier nur Dmitri Galuškevitš, welcher in Estland als Angreifer in Fall 3 identifiziert werden konnte. Alle anderen beteiligten Angreiferinnen und Angreifer aus Fall 3 konnten nicht identifiziert werden, weshalb Fall 3 auch nicht zu den Fällen gehört, wo die Angreiferin oder der Angreifer mit überwiegender Sicherheit identifiziert wurde. Die Autoren aus [64] haben bereits festgestellt, dass Cyber-Terroristinnen und Cyber-Terroristen der Eindruck vermittelt werden muss, man kann sie erwischen. Im Zuge der betrachteten Fälle konnte allerdings festgestellt werden, dass seitens der Terroristinnen und Terroristen diese Wahrnehmung noch nicht bestehen kann, zumindest basierend auf den Fakten, dass beinahe keine der Angreiferinnen beziehungsweise keiner der Angreifer wirklich mithilfe der Aufklärungsarbeiten ausgemacht werden konnte.

Eine abschließende Zusammenfassung der vorher genannten Fakten zu den Angreiferinnen und Angreifern bietet Tabelle 15: Kurzüberblick zu Täterinnen und Tätern von Cyber-Terrorismus. Tabelle 15 zeigt zunächst, ob die zugesprochene Täterin oder der zugesprochene Täter wahrscheinlich, nur erahnbar, oder beinahe gänzlich unklar ist. In der Spalte Aufklärung wird die Art und Weise, wie man primär zur Täterin oder zum Täter gelangt ist, beschrieben. Dies kann durch eine Bekennung oder eine Beweissicherung geschehen. Wenn die Täterin oder der Täter unbekannt ist, wird hier nichts eingetragen. Die Angriffsart beschreibt kurz, ob es sich um einen Angriff mit Störungen und/oder Schäden handelte oder, um reine Spionage ohne größer spürbare Ausfälle an den Systemen.

Nummer	Kurzbezeichnung	Täterin/Täter	Aufklärung	Angriffsart
1	Sri Lanka	Wahrscheinlich	Bekennung	Störung
2	Aum Shinrikyo	Wahrscheinlich	Beweissicherung	Spionage
3	Estland	Erahnbar	Bekennung/Beweissicherung	Störung
4	Georgien	Erahnbar	Beweissicherung	Störung
5	Vereinigte Staaten	Unbekannt	-	Spionage
6	Südkorea	Wahrscheinlich	Beweissicherung	Störung
7	Saudi-Arabien	Erahnbar	Bekennung	Störung
8	Ukrainie	Erahnbar	Beweissicherung	Störung
9	Israel	Wahrscheinlich	Beweissicherung	Störung[20]

Tabelle 15: Kurzüberblick zu Täterinnen und Tätern von Cyber-Terrorismus

Zuletzt soll in diesem Abschnitt noch nachgegangen werden, ob es eine gewisse Tendenz dazu gibt, wo die Angreiferinnen und Angreifer herkommen beziehungsweise wo die Angriffe zumindest nach dem Stand der Untersuchungen ihren wahrscheinlichsten Ursprung haben. Einen besseren Überblick bietet hier Abbildung 12: Weltübersicht Cyber-Terrorismus Angreiferinnen und Angreifer. In Abbildung 12 sind die Länder, aus denen die Angreiferinnen und Angreifer höchstwahrscheinlich stammen, farblich markiert. Nachdem es bei Fall 5 sehr wenige Informationen zu den Angreiferinnen oder Angreifern gibt, wurde hier kein Land markiert. Abbildung 12 zeigt, dass bei den gewählten Fällen von Cyber-Terrorismus alle Täterinnen und Täter im asiatischen Raum beheimatet sind. In Asien selbst gibt es eine klare Tendenz nach Russland, wo 3 der Fälle zugeordnet wurden. Es gibt zwar keine Beweise für einen Täter in Fall 5, aber der Verdacht geht wieder in den asiatischen Raum nach Russland beziehungswiese China. Im Gegensatz zu Russland führte bei keinem der behandelten Fälle die Spur nach China.

[20] Es gab zwar keine Störungen in Fall 9, aber es ist davon auszugehen, dass Hamas Störungen und Schäden verursachen wollte.

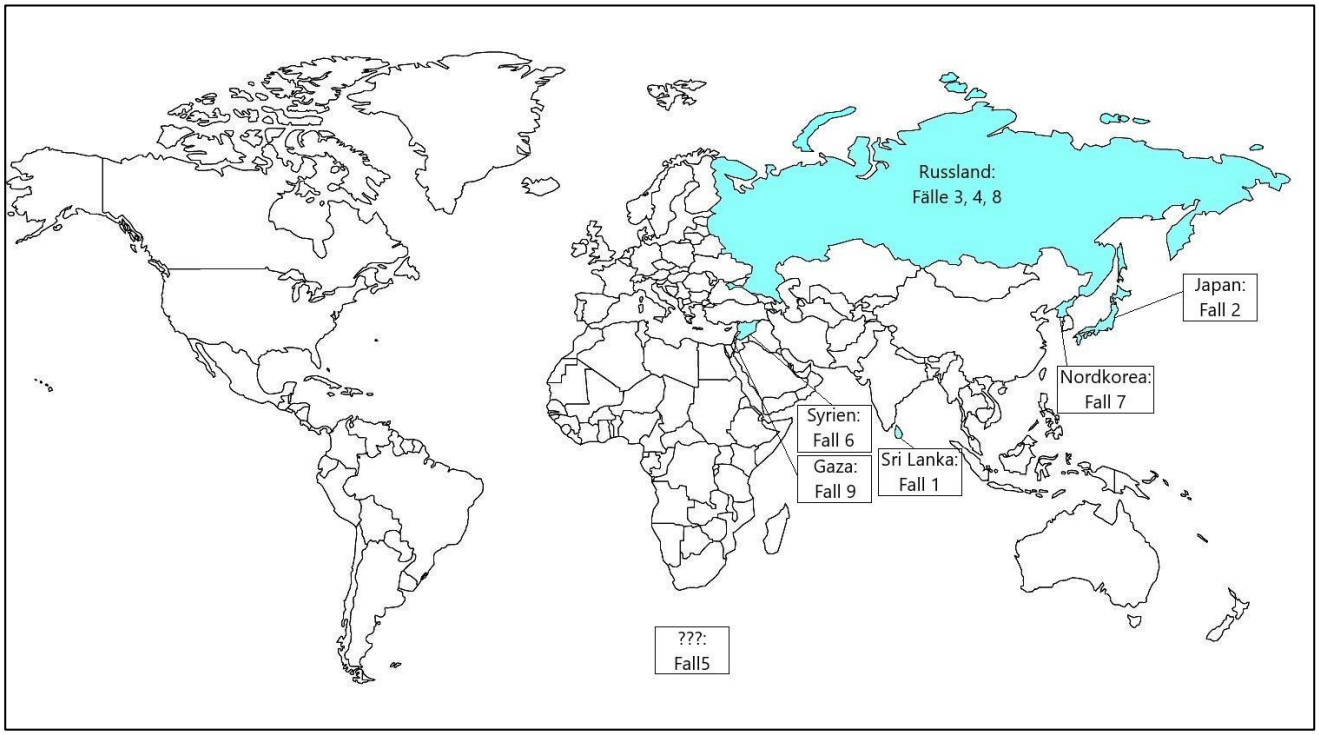


Abbildung 12: Weltübersicht Cyber-Terrorismus Angreiferinnen und Angreifer[21]

4.2. Ziel

Im Gegensatz zu den Täterinnen und Tätern sind die Opfer nach den Angriffen leichter festzustellen. Dies liegt an den merkbaren Schäden, die die terroristischen Angreiferinnen und Angreifer mit ihren Cyber-Operationen in den meisten Fällen verursacht haben. Anders ist es jedoch bei Fällen, die nur auf Informationsdiebstahl und Spionage abzielten. Solange hier das Opfer nichts von den Operationen der Angreiferin oder des Angreifers bemerkt kann es nicht als Ziel wahrgenommen werden. Beispiele dafür sind die Fälle 2 und 5. Bei Fall 2 in Japan gelang es nur durch eine Zufallskontrolle der Polizei die gestohlenen Daten sicherzustellen, an die Aum Shinrikyo durch den Vertrieb von Software gelangen konnte. Daher kann es sein, dass es ähnliche Fälle von Datenlecks gibt, die aber noch nicht entdeckt wurden. In Fall 5, welcher hauptsächlich die Energieversorgung in den Vereinigten Staaten betraf, wurde später bekannt, dass auch andere Dienstleister in den Vereinigten Staaten betroffen waren. Man entdeckte die Schadsoftware beispielsweise bei der Wasserversorgung und im Finanzwesen. Aufgrund fehlender Ausfälle könnte es hier weitere Ziele im Zuge dieser Cyberspionagekampagne gegeben haben, die noch nicht identifiziert wurden. Schließlich arbeitete man bereits zum Zeitpunkt der Bekanntgabe 2009 seit etwa zwei bis drei Jahren an der Entfernung der Schadsoftware. Bei den Angriffen auf Israel ist das Ziel der Öffentlichkeit ebenfalls nicht bekanntgegeben worden, da dies einen Nachteil für Israel in den Konflikten mit Hamas bedeuten könnte.

Um ein besseres Verständnis dafür entwickeln zu können, welche Ziele Terroristinnen und Terroristen für Cyber-Angriffe auswählen soll anhand der neun ausgewählten Fälle versucht werden eine Tendenz herauszuarbeiten, um welche Ziele es sich handelte. Um das zu erreichen wurde eine Kategorisierung der Ziele vorgenommen, die auf Ähnlichkeiten in den angebotenen Diensten und dem Tätigkeitsfeld basiert. Bei der Analyse der betroffenen Ziele in den neun Fällen konnten acht Kategorien festgestellt werden. Drei davon besitzen allerdings nur einen Eintrag und die Ziele sind damit allein in ihrer Kategorie. Die acht Kategorien und deren zugewiesen Anzahl an Zielen sind in Tabelle 16: Kategorien für Ziele gelistet und die Eigenschaften dieser Kategorien erklärt.

[21] Bild für die Weltkarte aus http://azausmalbilder.net/ausmalbild/426360 (Zugriff am 21.1.2020)

Kategorie	Eigenschaften	Anzahl
Regierungen	Das betroffene System wird von der Regierung betrieben oder es handelt sich um eine Regierungsperson, welche der Eigentümer des Ziels ist.	4
Kernenergie	Das betroffene Unternehmen arbeitet im Bereich der Kernenergie. Dazu gehören beispielsweise Kernkraftanlagen und Nukleareinrichtungen.	1
Banken	Dieser Kategorie wurden Unternehmen zugeordnet, die im Banken- und Finanzwesen aktiv sind.	3
Internet- und Telefondienstanbieter	Dazu gehören Anbieter von Kommunikationsanlagen.	4
Medien	Alle Betreiber von digitalen Medien, wie Zeitungen und Fernsehsender wurden in dieser Kategorie zusammengefasst.	3
Grundversorger	Hier werden die Betreiber von grundlegenden Services zusammengefasst. Das sind zum Beispiel Stromanbieter, Wasserversorger, aber auch Öl- und Gaslieferanten.	3
Mineralgewinnung und Verarbeitung	Eine Gruppe für Bergbaubetriebe.	1
Transportunternehmen	Eine Gruppe für Eisenbahnbetreiber.	1

Tabelle 16: Kategorien für Ziele

Fall	Ziel(e)	Kategorie
1	Botschaft in Südkorea, Kanada und den Vereinigten Staaten	Regierungen
2	Diverse Betreiber von Kernkraftanlagen und Nukleareinrichtungen, sowie Transportinformationen für Kernmaterial	Kernenergie
3	Verschiedene Webseiten der estnischen Regierung und Premierminister Estlands	Regierungen
	Banken	Banken
	Internet Service Provider	Internet- und Telefondienstanbieter
	Online Medien	Medien
4	Verschiedene Webseiten der georgischen Regierung, Präsident Georgiens und Botschaft der Vereinigten Staaten und des Vereinigten Königreichs	Regierungen
	Internet Service Provider Georgiens	Internet- und Telefondienstanbieter
	Webseiten von Fernsehsendern und Zeitungen	Medien
5	Betreiber der Stromversorgung, Wasserversorgung und Abwasseranlagen, sowie Öl- und Gaslieferanten	Grundversorger
	Telekommunikationsfirmen	Internet- und Telefondienstanbieter
	Finanzdienstleister	Banken
6	Verschiedene Webseiten der saudi-arabischen Regierung	Regierungen
7	Shinhan Bank, Nonghyup Bank und Jeju Bank	Banken
	Korean Broadcasting System, Munhwa Broadcasting Corporation und Yonhap Television News	Medien
	LG Uplus	Internet- und Telefondienstanbieter
8	Prykarpattiaoblenergo, Chernivtsioblenergo und Kyivoblenergo	Grundversorger
	Ukrainisches Bergbauunternehmen	Mineralgewinnung und Verarbeitung
	Ukrainischer Eisenbahnbetreiber	Transportunternehmen
9	Kritische zivile Infrastruktur	Grundversorger
	Sichere Kommunikationskanäle	Internet- und Telefondienstanbieter

Tabelle 17: Kategorisierung Ziele von Cyber-Terrorismus

Die betroffenen Ziele aus den neun Fällen werden in Tabelle 17: Kategorisierung Ziele von Cyber-Terrorismus nochmals kurz in einer Übersicht dargestellt. In der Spalte Fall wird hierbei die Nummer des entsprechenden Falls angegeben. Ziel(e) enthält eine Zusammenfassung der Ziele aus den neun Fällen. Teilweise wurden die Ziele zusammengefasst, um eine bessere Übersicht zu gewährleisten. In der letzten Spalte ist die zugewiesene Kategorie eingetragen. Durch diese Kategorisierung konnte aus den 20 Ziel(e)-Einträgen in Tabelle 17 eine Zusammenfassung aus acht Typen von Zielen erstellt werden. An der Spitze der gewählten Fälle stehen Regierungen und Internet- und Telefondienstanbieter, welche in vier der neun Fälle betroffen waren. Sowohl Banken als auch Medien und Grundversorger waren in drei der neun Fälle betroffen. Einzelfälle gab es in den Kategorien Kernenergie, Mineralgewinnung und Verarbeitung und bei Transportunternehmen. Mithilfe der betrachteten Fälle konnte die Feststellung von [25] bestätigt werden, dass militärische Einrichtungen nicht zu den bevorzugten Zielen von Terroristen gehören. In den betrachteten Fällen finden sich primär keine Aufzeichnungen zu Cyber-Angriffen auf militärische Einrichtungen.

Ähnlich wie in Kapitel 4.1 Angreifer sollen auch die Herkunftsländer der Ziele genauer betrachtet werden. Dieser Überblick findet sich in Abbildung 13: Weltübersicht Cyber-Terrorismus Ziele. Darin ist zu sehen, dass die Ziele viel mehr über den Globus verteilt sind, als die Angreiferinnen und Angreifer, die in den gewählten Fällen alle aus Asien operierten. Es stehen allerdings auch 20 Ziele neun Angreiferinnen und Angreifern gegenüber. Die Ziele finden sich nunmehr in Nordamerika, Europa und Asien. Keine Ziele in der Stichprobe gab es in Afrika, Australien und Südamerika. Am häufigsten Opfer von Cyber-Terrorismus sind die Vereinigten Staaten und Südkorea mit jeweils drei Fällen gewesen. Die Ukraine ist ebenfalls zwei Mal innerhalb der behandelten Fälle von Cyber-Terrorismus betroffen gewesen. Auch in weiteren zehn Ländern ist Cyber-Terrorismus aufgetreten. Der japanische Kult Aum Shinrikyo schaffte es im Zuge seiner Cyberspionageaktionen Informationen von insgesamt fünf verschiedenen Ländern zu erlangen. Durch Angriffe auf Botschaften schafften es die Liberation Tigers of Tamil Eelam in Fall 1 und die Angreiferinnen und Angreifer in Georgien bei Fall 4 drei Länder gleichzeitig zu Zielen zu machen.

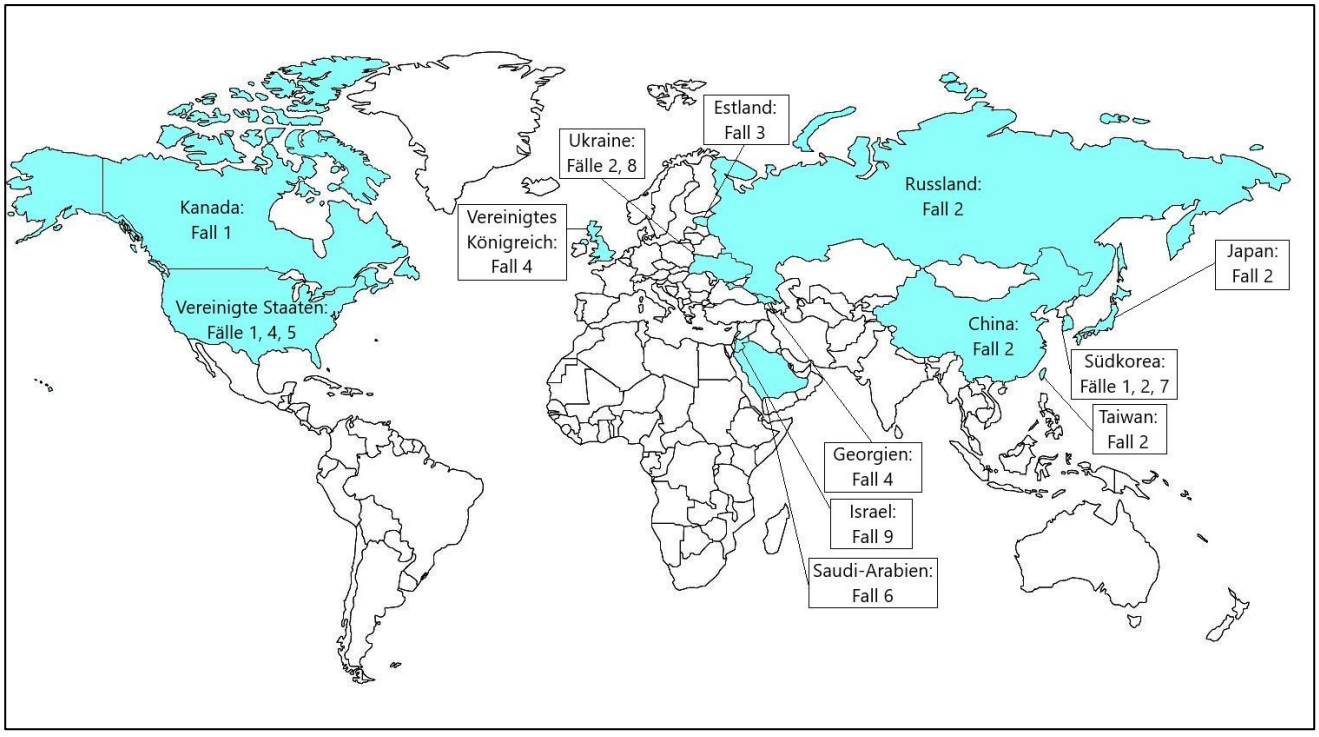


Abbildung 13: Weltübersicht Cyber-Terrorismus Ziele[22]

[22] Bild für die Weltkarte aus http://azausmalbilder.net/ausmalbild/426360 (Zugriff am 21.1.2020)

4.3. Angriff

In den neun ausgewählten Fällen von Cyber-Terrorismus nutzten die Täterinnen und Täter mehrere Angriffsmöglichkeiten, um mehr oder weniger erfolgreich gegen ihre Opfer vorzugehen. In diesem Abschnitt sollen diese Angriffsarten in einer Übersicht dargestellt werden, um festzustellen, welche Angriffsarten am häufigsten genutzt wurden. Diese Übersicht soll anschließend in Kapitel 4.4 Folgen genutzt werden um die Effektivität, also die Stärke der Auswirkungen anhand der Angriffsarten zu bewerten. Außerdem sollen die eingesetzten Angriffsarten hinsichtlich Umfang und erforderlicher Kenntnisse so gut wie möglich bewertet werden, um besser abschätzen zu können, welcher Aufwand von Seiten der Terroristinnen und Terroristen entsteht.

Die Übersicht der Angriffe findet sich in Tabelle 18: Übersicht Angriffsarten von Cyber-Terroristinnen und Cyber-Terroristen. Tabelle 18 beinhaltet zunächst die Fallnummer in der Spalte Fall. Eine Kategorisierung des Angriffs ist in der Spalte Angriff(e) zu finden. In jedem der neun Fälle ist der Detailgrad, wie die Angriffe verlaufen sind unterschiedlich. Um die Fälle besser vergleichen zu können, handelt es sich bei Angriff(e) um eine Verallgemeinerung. Wie diese Kategorisierung entstanden ist wird in der Spalte Zusatzinformationen erläutert, welche sich Großteils auf den Abschnitt Angriff beim jeweiligen Fall bezieht, aber auch Informationen aus den anderen drei Abschnitten zur Schlussfolgerung heranzieht.

Fall	Angriff(e)	Zusatzinformationen
1	Denial of Service	Die E-Mail-Server wurden mit zahlreichen E-Mails geflutet, die sie nicht mehr bearbeiten konnten und den Dienst verweigerten.
2	Social Engineering	Die Terroristinnen und Terroristen von Aum Shinrikyo haben sich als Softwareentwickler ausgegeben und im Zuge ihrer legalen Arbeiten Informationen abgegriffen.
3	Denial of Service	Im Zuge der Angriffe wurden Methoden wie ICMP Flooding und UDP Flooding eingesetzt und so ein Denial of Service der betroffenen Geräte verursacht. Des Weiteren wurde der Mailserver der Regierung übernommen und sendete zahlreiche falsche Nachrichten.
	SQL-Injektion	Es gibt Berichte zu Versuchen mit SQL-Injektionen.
4	Denial of Service	Der Großteil der Angriffe bestand darin Webseiten in Georgien nicht mehr verfügbar zu machen.
	SQL-Injektion	Mithilfe von SQL-Injektionen wurden einige Webseiten manipuliert.
	Cross-Site Scripting	Auch Cross-Site-Scripting zählte zu den Angriffen.
	Schadsoftware	In geringem Ausmaß wurde Schadsoftware an die Ziele verteilt.
5	Schadsoftware	In den Vereinigten Staaten kämpfte man mit einer Schadsoftware.
6	Phishing	Die Syrian Electronic Army verunstaltete einige Webseiten der saudi-arabischen Regierung. Zu ihren Angriffsarten gehören üblicherweise Social Engineering, Phishing und Distributed Denial of Service Angriffe. Nachdem die Webseiten verunstaltet wurden haben sie vermutlich mithilfe einer Phishing-Mail Zugang zu den Servern erlangen können.
7	Phishing	Mithilfe einer Phishing-Mail konnten die Angreiferinnen und Angreifer eine Präsenz auf den Systemen etablieren.
	Schadsoftware	Die Phishing-Mail enthielt den Installer für einen Trojaner, der den Angreiferinnen und Angreifern einen Remote Zugriff erlaubte.
8	Phishing	Mithilfe einer Phishing-Mail konnten die Angreiferinnen und Angreifer eine Präsenz auf den Systemen etablieren.
	Schadsoftware	Der Fall dreht sich Großteils um die Malware Black Energy.
	Denial of Service	Die Telefonanlagen des Supports wurden mit Anrufen überflutet (Telefon Denial of Service)
9	Keine Angaben	Da es keine Informationen in Fall 9 gibt, kann ihm kein Angriff zugeordnet werden.

Tabelle 18: Übersicht Angriffsarten von Cyber-Terroristinnen und Cyber-Terroristen

Die meisten unterschiedlichen Angriffe konnten im Fall 4 in Georgien festgestellt werden. Immerhin drei Angriffsarten waren es bei Fall 8 in der Ukraine. In Estland und Südkorea nutzten die Angreiferinnen und Angreifer zwei Angriffsmöglichkeiten. Weniger umfangreich waren die Fälle 1, 2, 5 und 6 wo man nur auf einem Weg im Cyber-Bereich versuchte das Ziel anzugreifen. Aufgrund zurückgehaltener Informationen in Fall 9 konnte hier nicht festgestellt werden welcher Angriffsweg von den Angreiferinnen und Angreifern gewählt wurde.

Am häufigsten eingesetzt wurden Denial of Service Angriffe und Schadsoftware. Beides konnte in zumindest vier der neun Fälle nachgewiesen werden. Auch Phishing ist eine beliebte Methode mit drei Einsätzen in unterschiedlichen Fällen gewesen. Versuche mit SQL Injections zählen in zwei der Fälle zu den Angriffsarten. Eher selten wurden Methoden wie Social Engineering und Cross Site Scripting gewählt. Beides wurde nur in jeweils einem Fall eingesetzt.

Nicht alle Angriffe waren gleich erfolgreich und manche blieben eher bei Versuchen, während andere das gewünschte Ziel der Terroristinnen und Terroristen vermutlich ganz gut erreichten. Aus diesem Grund soll eine weitere Tabelle die Erfolge der Angriffsmöglichkeiten aus Tabelle 18 mithilfe der gewonnenen Informationen aus Kapitel 3 darstellen. Diese Bewertung ist in Tabelle 19: Angriffserfolge nach Art dargestellt. Angriff beinhaltet die Angriffsart und Informationen die verfügbaren Details, wie groß die Erfolge dieser Angriffsmethode waren. Die abschließende Bewertung erfolgt in den Möglichkeiten wenig erfolgreich, teilweise erfolgreich und übermäßig erfolgreich. Wenig erfolgreich wird vergeben, wenn der Angriff keinen oder nur wenig Erfolg hatte, teilweise erfolgreich, wenn es Fälle mit und ohne Erfolg gab und übermäßig erfolgreich, wenn die Angriffsmethode ihr vermeintliches Ziel erreicht hat. Tabelle 19 zeigt, dass beinahe alle Angriffsarten Erfolg hatten und nur die einfachen Versuche der Angreifer in Georgien mithilfe von Malware scheiterten. In den Vereinigten Staaten ist es schwer zu sagen wie erfolgreich die Aktionen aus Sicht der Angreiferinnen und Angreifer waren, da es nicht nachvollziehbar ist, an welche Informationen sie gelangen konnten und welchen Vorteil sie jetzt dadurch haben.

Angriff	**Informationen**	**Bewertung**
Denial of Service	In den Fällen 1, 3, 4 und 8 konnte ein Denial of Service ziemlich erfolgreich für zumindest einige Zeit die betroffenen Services behindern und ist somit als erfolgreich zu betrachten.	übermäßig erfolgreich
Schadsoftware	In Fall 4 zu Georgien war die vereinzelt verteilte Malware nicht erfolgreich, da sie zu leicht erkennbar war. Nachdem in Fall 5 in den Vereinigten Staaten auch nicht wirklich mit Ausfällen zu kämpfen war und nicht bekannt ist wie erfolgreich die Spionage war ist hier kein großartiger Erfolg zu verzeichnen. Anders ist das in den Fällen 7 (Südkorea) und 8 (Ukraine), wo die Malware große Schäden und Ausfälle verursachte.	teilweise erfolgreich
Phishing	Es ist zwar nicht ganz sicher, ob in Fall 6 mittels Phishing die Zugangsdaten für die Webserver erlangt werden konnten, aber in den Fällen 7 und 8 war es eine sehr erfolgreiche Methode, um eine erste Präsenz auf den angegriffenen Systemen etablieren zu können.	übermäßig erfolgreich
SQL-Injektion	Sowohl in Estland als auch Georgien wurden SQL Injections genutzt, um beispielsweise das Aussehen von Webseiten zu verändern. Diese Angriffe waren seitens der Angreiferinnen und Angreifer erfolgreich.	übermäßig erfolgreich
Social Engineering	Zumindest im Falle von Aum Shinrikyo war die Zusammenarbeit mit Firmen erfolgreich und die Opfer ahnten nichts von den eigentlichen Absichten ihrer geschäftlichen Partner.	übermäßig erfolgreich
Cross Site Scripting	Die Berichte über den Einsatz von Cross-Site Scripting bei Fall 4 sprechen für einen erfolgreichen Angriff.	übermäßig erfolgreich

Tabelle 19: Angriffserfolge nach Art

Zuletzt soll in diesem Kapitel noch darauf eingegangen werden, wie schwierig beziehungsweise aufwändig die einzelnen Angriffsarten sind. Das Hauptaugenmerk soll hierbei vor allem auf organisatorischen Aspekten liegen.

Wenn man zunächst die Angriffe rund um einen Denial of Service betrachtet, sind diese nicht sehr schwierig umzusetzen, da man beispielsweise nur einen Server mit sehr vielen Anfragen überhäufen muss. Etwas mehr Organisationsaufwand entsteht beim Distributed Denial of Service Angriff, wenn zumindest zwei Personen die Anfragen gleichzeitig an den Server schicken. das kann zum Beispiel, wie in Fall 3 in Estland, über ein Forum gemacht werden, wo nicht nur erklärt wird, wie man den Angriff startet, sondern auch festlegt, wann in etwa gestartet werden soll (vergleiche Abbildung 8 beziehungsweise 9). Eine andere Möglichkeit für den Distributed Denial of Service ist das Botnet. Ein Botnet zu betreiben erfordert jedenfalls mehr technisches Wissen als ein einfacher Denial of Service Angriff, den nur eine Person ausführt. Schließlich müssen fremde Endgeräte übernommen und dann für den Angriff missbraucht werden können.

Die Entwicklung von Schadsoftware erfordert Programmierkenntnisse. Das ist zwar noch nicht das große Problem, aber es darf sich nicht um zu einfach entwickelte Malware handeln, da Erfolge sonst ausbleiben, wie sich in Georgien (Fall 4) gezeigt hat. Sehr erfolgreich war auch Phishing und der Abgriff von Benutzerinformationen. Dafür benötigt es nicht viel, da man das Opfer nur mit seriös wirkenden Nachrichten dazu bringen muss Login-Informationen oder Ähnliches, was für den Zugang zum Zielsystem benötigt wird, preiszugeben. Eher einfach wird es für die Angreiferin oder den Angreifer auch bei SQL-Injektionen, da sie beziehungsweise er hierfür ebenfalls keine Koordination mit anderen Personen braucht und nur lange genug bei Eingabefeldern versuchen muss den gewünschten Input durch die Sicherheitsmaßnahmen zu bringen. Eine sehr große Organisation lag im einzigen Social Engineering Fall der Stichprobe vor. Aum Shinrikyo erschlich sich das Vertrauen der betroffenen Firmen, indem eigene Firmen zur Softwareentwicklung gegründet wurden. Der Einsatz von Cross Site Scripting ist ähnlich zur Verwendung von Malware. Hier werden entsprechende Scripting Kenntnisse gebraucht.

Für alle eingesetzten Angriffsarten braucht man ein Endgerät mit Internetanschluss. Prinzipiell kann der Social Engineering Angriff ausgenommen werden, aber wenn man erbeutete digitale Daten abrufen möchte ist zumindest das Endgerät von Nöten. Manchmal ist zusätzlich zu Endgerät und Internetanschluss noch etwas technisches Wissen erforderlich um Angriffe, wie zum Beispiel Cross Site Scripting oder die Installation von Schadsoftware durchführen zu können. Trotzdem kann abschließend die Bilanz gezogen werden, dass Angriffe relativ einfach durchgeführt werden können und wenig Hardware voraussetzen.

4.4. Folgen

Im letzten Teil der Zusammenfassung der Fälle soll eine Übersicht der Folgen von Cyber-Terrorismus entstehen. Diese Folgen sollen im Zusammenhang mit den eingesetzten Angriffsmethoden aus Kapitel 4.3 Angriff (siehe Tabelle 18 und Tabelle 19 Spalte Angriff) verglichen werden. Diese Übersicht wurde in Tabelle 20: Folgen von Cyber-Terrorismus nach Angriffsarten dargestellt.

Insgesamt betrachtet liefert Tabelle 20 unterschiedliche Folgen von Cyber-Terrorismus. Es reicht von hauptsächlich finanziellen Schäden in Estland, über teilweise negative Propaganda in Georgien bis hin zu Verlusten in der Lebensqualität in der Ukraine, wo die Bevölkerung unter Stromausfällen zu leiden hatte. Prinzipiell hatte vermutlich jeder der Angriffe nachträglich finanzielle Auswirkungen, da man entsprechende Wiederherstellungsarbeiten durchführen musste und unter Umständen in weitere Sicherheitsmaßnahmen investierte um zukünftige Angriffe verhindern zu können.

Direkte Auswirkungen für die Bevölkerung waren vor allem in der Ukraine, Estland und Georgien spürbar. Obwohl in Georgien die Situation durch den Krieg mit Russland nicht nur auf Cyber-Terrorismus beruht. Die Unterbrechung der Kommunikation sorgte in der Ukraine für eine längere Reaktionszeit, während sie in den betroffenen Botschaften aus Fall 1 die Kommunikation von Botschaftern störte. Mit fehlender Information von Nachrichten und Regierung, verursacht durch Ausfälle der Internetinfrastruktur, musste man vor allem in Estland, Georgien und Saudi-Arabien zurechtkommen. Wenige negative Auswirkungen sind vergleichsweise dazu bei den Fällen 2, 5 und 9 bekannt, was auf reine Spionage beziehungsweise schnelle Reaktion zurückzuführen ist.

Fall	Angriff	Folgen
1, 3, 4, 8	Denial of Service	Mithilfe von Denial of Service Angriffen konnte die Kommunikation blockiert werden, indem Mailserver (Fall 1) und Telefonanlagen (Fall 8) nicht mehr ordnungsgemäß funktionierten. Außerdem gelang es Informationen nicht mehr abrufbar zu machen, da die entsprechenden Webserver nicht mehr erreichbar waren. In Estland entstanden außerdem Schäden für alle betroffenen Unternehmen, die ihre Services nicht mehr anbieten konnten und auf eine funktionierende Internetinfrastruktur angewiesen waren.
4, 5, 7, 8	Schadsoftware	Die Folgen von Schadsoftware hielten sich in Fall 4 (Georgien) stark in Grenzen und man kann nicht wirklich von Ausfällen sprechen. Fall 5 (Vereinigte Staaten) bleibt schwer zu beurteilen, aber für die Bevölkerung selbst entstanden keine spürbaren Folgen der Malware. Etwas anders ist das bei Fall 7 (Südkorea), wo tatsächlich Ausfälle betroffener Services entstanden sind. Diese dauerten aber nur etwa einen Tag an und wirtschaftliche Schäden entstanden vor allem bei den Betreiberinnen und Betreibern selbst. Ähnlich getroffen wurde ein Teil der Bevölkerung der Ukraine, die etwa einen Tag ohne Strom auskommen musste.
6, 7, 8	Phishing	Nachdem die Webseiten Saudi-Arabiens nicht mehr erreichbar waren, konnten Informationen und Services nicht mehr genutzt werden. In den Fällen 7 und 8 galt Phishing als Wegbereiter und die eigentlichen Schäden, die schlussendlich entstanden, sind jene aus der Zeile Schadsoftware.
3, 4	SQL-Injektion	In Estland entstanden durch SQL-Injektionen ähnliche Ausfälle wie durch Denial of Service Angriffe. In Georgien führten sie zur Verunstaltung von Webseiten.
2	Social Engineering	Welches Potential die erbeuteten Informationen für Aum Shinrikyo gehabt hätten, lässt sich nur erahnen. Trotzdem handelt es sich um Offenlegung vertraulicher Informationen.
4	Cross Site Scripting	Analog zu den Angriffen mit SQL-Injektionen konnte mit Cross Site Scripting das Aussehen von Webseiten verändert werden.

Tabelle 20: Folgen von Cyber-Terrorismus nach Angriffsarten

4.5. Frameworks zur Beschreibung von Cyber-Bedrohungen

In jedem der betrachteten neun Fälle sind Aufzeichnungen in unterschiedlichen Detailgraden vorhanden. Dadurch lassen sich unterschiedlich viele Informationen aus jedem Fall entnehmen, die anschließend dazu genutzt werden können in zukünftigen Fällen präventive Maßnahmen zu setzen (siehe Kapitel 5). Es gibt bereits bestehende Frameworks zu Cyber-Bedrohungen, die bestimmte Aspekte vordefinieren, welche man bei einem Cyber-Angriff betrachten kann. Beispielhaft wurde das Framework STIX (Structured Threat Information Expression) ausgewählt, um zwei Fälle in der vorgegebenen Form von STIX zu beschreiben. Bei den zwei Fällen handelt es sich um die Fälle 3 und 8, da sie im Vergleich mit anderen Fällen viele Informationen liefern.

Das STIX-Framework wurde ausgewählt, da STIX bereits zur allgemeinen Beschreibung von Cyber-Angriffen genutzt werden kann. Die darin enthaltenen vordefinierten Attribute lassen sich mit einigen Aspekten, die im Zuge der neun Fälle von Cyber-Terrorismus betrachtet wurden, vereinbaren. So wurde beispielsweise für den Angreifer der Threat Actor gewählt, die beschrieben Angriffsmethoden unter Angriff wurden entsprechend zu STIX in die Objekte Attack Pattern, Malware und Tool zugeordnet. Im Zuge der Arbeiten wurde STIX-Version 2.0 und die dazugehörige Dokumentation aus [171] verwendet. Zur Modellierung wurde zusätzlich ein STIX-Editor herangezogen, welcher frei unter [172] verfügbar ist.

Vor der Beispielimplementierung soll noch kurz genauer auf alle Attribute des STIX-Frameworks eingegangen werden. STIX 2 definiert zwölf STIX Domain Objects, die in Tabelle 21 STIX Domain Objects und Relationship Objects [171] aufgelistet sind. Object in Tabelle 21 zeigt eine Grafik des Objekts, das später in der Visualisierung genutzt wird. Der Name ist eine kurze Bezeichnung für das Objekt. Zuletzt befindet sich in Tabelle 21 noch eine Kurzbeschreibung des Domain Objects beziehungsweise Relation Objects laut [171].

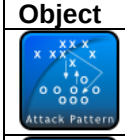
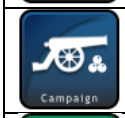
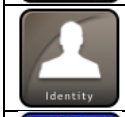
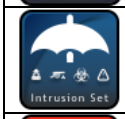
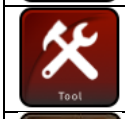
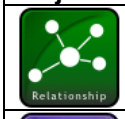
Domain Objects		
Object	**Name**	**Kurzbeschreibung**
	Attack Pattern	A type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets.
	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks that occur over a period of time against a specific set of targets.
	Course of Action	An action taken to either prevent an attack or respond to an attack.
	Identity	Individuals, organizations, or groups, as well as classes of individuals, organizations, or groups.
	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
	Intrusion Set	A grouped set of adversarial behaviors and resources with common properties believed to be orchestrated by a single threat actor.
	Malware	A type of TTP, also known as malicious code and malicious software, used to compromise the confidentiality, integrity, or availability of a victim's data or system.
	Observed data	Conveys information observed on a system or network (e.g., an IP address).
	Report	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details.
	Threat Actor	Individuals, groups, or organizations believed to be operating with malicious intent.
	Tool	Legitimate software that can be used by threat actors to perform attacks.
	Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.
Relationship Objects		
Object	**Name**	**Kurzbeschreibung**
	Relationship	Used to link two STIX Domain Objects and to describe how they are related to each other.
	Sighting	Denotes the belief that an element of cyber threat intelligence was seen (e.g., indicator, malware).

Tabelle 21 STIX Domain Objects und Relationship Objects [171]

Beginnend bei Estland (Fall 3) ist eine mögliche Beschreibung des Falls mithilfe von STIX in Anhang A ersichtlich. Der entstandene Code im .json Format wurde anschließend mithilfe eines STIX-Visualisierungstools [173] in eine Grafik umgewandelt (Abbildung 14: STIX-Visualisierung Estland). Grundsätzlich ist mithilfe von

STIX eine Beschreibung der wesentlichen Inhalte des Angriffs auf Estland möglich. Was nur schwer abzubilden ist, sind beispielsweise Anleitungen im Internet, so wie es in Estland der Fall war. Dies ist nicht unbedingt etwas einmaliges, da bei den Angriffen auf Georgien eine Liste mit möglichen Zielen veröffentlicht wurde. Beide Onlineressourcen sind nicht unmittelbar in STIX beschreibbar.

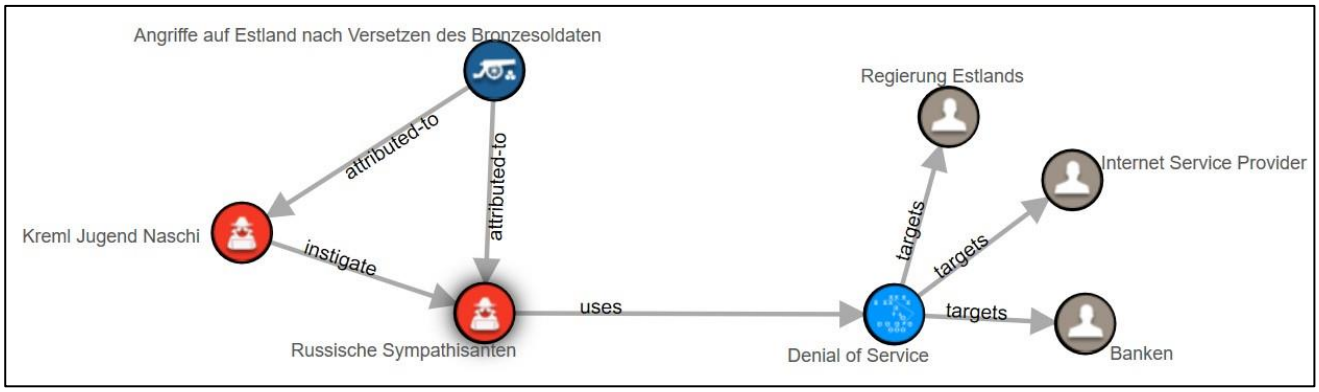


Abbildung 14: STIX-Visualisierung Estland

Die STIX-Modellierung des Angriffs auf die drei Stromversorger der Ukraine (siehe Anhang A) wurde wie im Fall von Estland zunächst in STIX erstellt und anschließend mit dem gleichen Tool [173] visualisiert (Abbildung 15: STIX-Visualisierung Ukraine). Im Vergleich zu Estland konnten mehr angebotene Attribute von STIX genutzt werden, um den Fall zu beschreiben. Auch hier sind die wesentlichen Informationen zum Fall aus der STIX-Version zu entnehmen. Alle zusätzlichen Informationen (zum Beispiel exakter Angriffshergang) könnten in die Attribute von STIX integriert werden, worauf aber in dieser beispielhaften Implementierung verzichtet wurde, um den Code kurz zu halten und nur die wesentlichsten Informationen zu inkludieren.

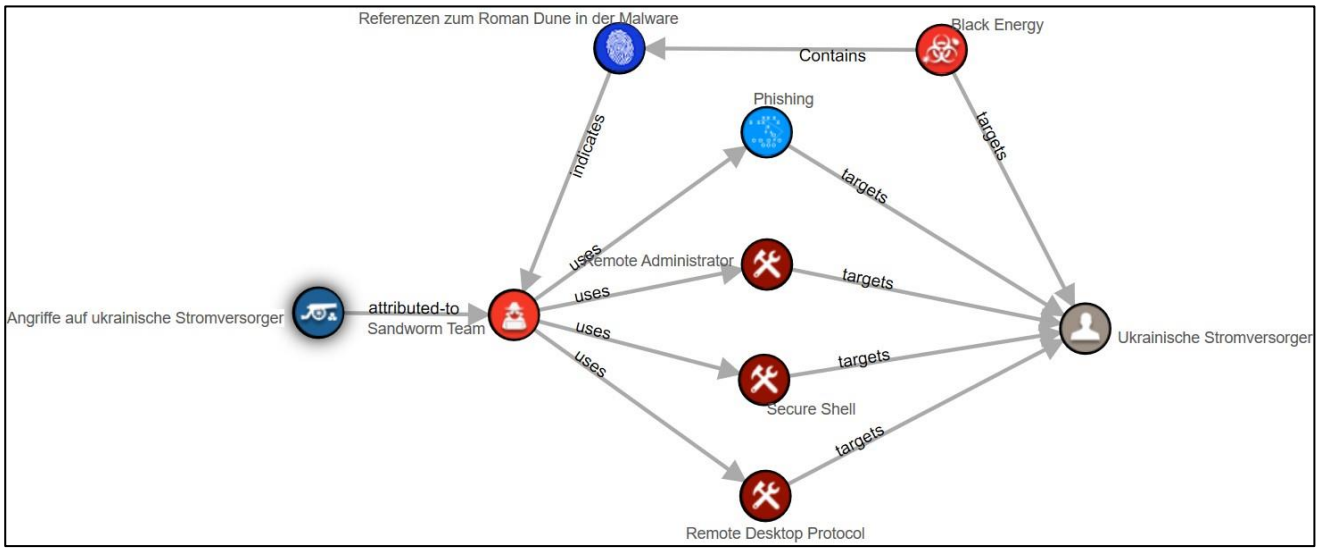


Abbildung 15: STIX-Visualisierung Ukraine

5. Prävention von Cyber-Terrorismus

In diesem Kapitel sollen auf Basis der gewonnen Informationen von den behandelten Fällen von Cyber-Terrorismus Maßnahmen abgeleitet werden, die aus kriminologischer Sicht die Attraktivität eines potenziellen Angriffsziels reduzieren, um einen Angriff durch Cyber-Terroristinnen und Cyber-Terroristen zu vermeiden beziehungsweise zu verhindern. Neben den Informationen aus den neun beschrieben Fällen von Cyber-Terrorismus aus Kapitel 3, sollen bereits bestehende Maßnahmen aus der Literatur herangezogen und bewertet werden. Abschließend zu diesem Kapitel soll eine Übersicht an Maßnahmen zur Vermeidung von Cyber-Terrorismus entstehen, die ähnlich zu [81] (vergleiche mit Tabelle 7: 25 Techniken für Situational Crime Prevention [81]) Techniken zur Prävention von Cyber-Terrorismus bietet.

Prinzipiell werden in der Arbeit von [81] zwei Modelle erwähnt, nämlich die Rational Choice Perspective und die Situational Crime Prevention. Weitere Details zu den beiden Modellen sind in Kapitel 2.7 Kriminologische Ansätze beschrieben. Diese Arbeit soll nicht nach Ursachen suchen, warum Terroristen ein gewisses Ziel ausgesucht haben, wie es die Rational Choice Perspective beschreibt (vergleiche mit Ursachen, wie zum Beispiel Nutzen oder „Joyriding“). Primär soll vermieden werden, dass der Angriff überhaupt passiert beziehungsweise zumindest die Auswirkungen reduziert werden. Dafür soll das Modell der Situational Crime Prevention aufgegriffen werden. So wie [81] 25 Techniken zur Vermeidung von Kriminalität in der realen Welt präsentiert, sollen Techniken aufgelistet werden, die Cyber-Terrorismus verhindern. Das Ergebnis befindet sich abschließend in diesem Kapitel in Tabelle 22: Techniken zur Vermeidung von Cyber-Terrorismus.

Zum besseren Verständnis, wie die Techniken ausgewählt wurden gibt es zu jeder der 20 Techniken eine kurze Erklärung. Das gleiche gilt auch für die Kategorien Erhöhen des Aufwands, Erhöhen der Risiken, Verringern des Erfolgs und Provokation verringern, die von den originalen Kategorien[23] aus [81] abgeleitet beziehungsweise übersetzt und angepasst wurden. Es wurden keine Maßnahmen im Bereich „Remove excuses“. beschrieben, da es aus den Fällen nicht unmittelbar ersichtliche Techniken gibt, die zu einer erfolgreichen Vermeidung eines cyber-terroristischen Angriffs führen. Nachdem [77] das Modell bereits in seiner Arbeit aufgegriffen hat und auf Cyberkriminologie angepasst hat fließen Ideen aus dieser Arbeit in Tabelle 22 ein.

Die ersten fünf Techniken sollen den Aufwand für die Angreiferin oder den Angreifer erhöhen. Dadurch soll erreicht werden, dass man mehr Zeit und Aufwand investieren muss, um erfolgreich zu sein.

1. Hardening: Zum Vermeiden von erfolgreichen Cyber-Angriffen ist ein Hardening der eingesetzten Systeme von Vorteil. Wie in den neun Fällen gezeigt sollte das Hauptaugenmerk darauf liegen sich vor allem gegen Denial of Service Angriffe und Malware zu schützen (vergleiche zum Beispiel Fall 8 Ukraine). Andererseits sollten Mitarbeiterinnen und Mitarbeiter, sowie Geschäftspartnerinnen und Geschäftspartner überprüft werden, bevor sie mit Arbeiten an Systemen betraut werden. Dies wurde von [77] empfohlen und zeigt auch im Fall von Aum Shinrikyo, dass es vor Angriffen schützen kann.
2. Servicezugriffe: Im Fall 8 in der Ukraine konnten die Angreiferinnen und Angreifer mithilfe gestohlener Benutzerinformationen auf die Systeme in den Umspannwerken zugreifen. Um dies zu verhindern können Maßnahmen wie beispielswiese die von [77] angeführte Multifaktorauthentifizierung helfen.
3. Die Überprüfung von Ausgängen ist für den Cyberraum nicht anwendbar. Eine Überprüfung der Ausgänge auf physischer Ebene kann aber funktionieren. Dafür benötigt es Personal am Ausgang, welches Personen beim Verlassen des Gebäudes hinsichtlich versuchten Diebstahls von Informationen durchsucht.
4. Straßensperren, getrennte Toiletten und die Verteilung von Pubs, wie von [81] angeführt, lassen sich nicht unmittelbar für den Cyber-Raum übertragen. Eine mögliche Adaptierung wäre das Ganze auf die bereitgestellten Services eines Unternehmens oder einer Regierung zu übertragen. Die betrachteten Fälle haben aber gezeigt, dass eine Separierung von Services auf verschiedene Internetseiten nicht funktioniert, da beispielsweise in Estland, Georgien und Saudi-Arabien trotzdem mehrere Regierungs-Webseiten angegriffen wurden, die unterschiedliche Services betrieben. Aus technischer Sicht könnte es sich allerdings teilweise um den gleichen physischen Server gehandelt haben, der mehrere Webseiten hostet, aber das sieht der Angreifer nicht im ersten Moment. [77] führt die Möglichkeit an physische Trennung durchzuführen. Im behandelten Fall von [77] konnte der Mitarbeiter auf die

[23] [81] verwendete die Begriffe „Increase the effort“, „Increase the risks“, „Reduce the rewards“, „Reduce provocation“, „Remove excuses“.

Computer seiner Kollegen aus einem anderen Funktionsbereich zugreifen. In Fall 2 war dies für Aum Shinrikyo aber kein Grund dennoch Versuche zu starten an mehreren physischen Standorten Informationen abzugreifen. Die Informationen können in diesem Fall aber mithilfe von manipulierter Software beschaffen worden sein. Jedenfalls erschwert aber eine Servicetrennung auf physischer Ebene gegen physische Angriffe helfen, wie von [77] beschrieben.

5. Hauptwerkzeug einer Cyber Terroristin oder eines Cyber-Terroristen ist ein Zugang zum Internet. Wenn man keinen Zugang zum Internet hat, kann man Angriffe nicht durchführen. Eine Umsetzung dieser Sperre läuft aber darauf hinaus, dass Internetserviceprovider Kundinnen und Kunden vorab und regelmäßig überprüfen müssen und bei potenzieller Gefährdung keine Services für die Person anbieten dürfen. Dies ist mit einigem zusätzlichen Aufwand verbunden und möglicherweise schwer realisierbar. Eine andere Möglichkeit wäre das Verkaufsverbot von internetfähigen Geräten an Kundinnen und Kunden, die potenzielle Absichten von Cyber-Terrorismus haben. Eine derartige Überprüfung führt aber zu ähnlichen Aufwänden wie das Verbieten der Internetverbindung.

Die nächsten fünf Techniken sollen das Risiko für Die Angreiferin oder den Angreifer erhöhen, dass sie oder er erwischt wird. Vor allem in diesem Bereich gibt es noch sehr viel Potenzial, wie die behandelten neun Fälle gezeigt haben.

6. Das Teilen von Informationen nach einem Vorfall hilft in der Aufklärung. Nachdem in Fall 5 (Vereinigte Staaten) eher wenige Umstände über die Angriffe bekannt sind, kann man ihn nicht mit anderen Angriffen vergleichen und Zusammenhänge erkennen. In Fall 7 (Südkorea) wurde mit McAfee zusammengearbeitet und dadurch Ähnlichkeiten zu vorhergehenden Angriffen gefunden. Auch im Falle der Ukraine (Fall 8) konnten Analysen Spuren zu bekannten Hacker-Gruppierungen ausmachen.
7. Eine natürliche Überwachung findet im Internet nicht statt. Wenn es um physische Sicherheit geht, sind die angeführten Maßnahmen sicherlich hilfreich, nicht aber im Cyber-Raum. Da die Angreiferin oder der Angreifer sich den Ort und Zeitpunkt des Angriffs beinahe beliebig aussuchen kann, soll statt diesem Punkt auf die automatische/toolbasierte Reduzierung der Anonymität gesetzt werden. Diese kann zum Beispiel mithilfe von verschiedenen Tracking-Technologien funktionieren. In den betrachteten Fällen hat das aber nur bedingt funktioniert, da zum Beispiel bei Fall 7 in Südkorea die IP-Adresse des Angreifers nicht zu ihm geführt hat. Etwas anders war das bei Fall 3, wo der Angreifer innerhalb Estlands ausgemacht und erwischt werden konnte.
8. Wenn es möglich wäre die Anonymität im Internet aufzuheben wäre die Aufklärungsquote vermutlich höher, als sie in den neun Fällen gewesen ist. Eine Möglichkeit ist, dass man seitens der Betreiber von Webservern beispielsweise von den Benutzern verlangt sich zu registrieren, bevor sie auf die eigentlichen Services zugreifen können. Diese Registrierung muss aber umfangreicher sein als die bloße Angabe einer E-Mail-Adresse, sondern sollte beispielsweise noch eine registrierte Telefonnummer erfordern, damit die Anonymität hier reduziert wird.
9. Wie schon von [77] angeführt kann man eine manuelle Überwachung durchführen, wie das Überprüfen von Logdateien. Eine Belohnung für das Melden von Auffälligkeiten, wie von [81] vorgeschlagen, könnte zu mehr und früher gemeldeten Vorfällen führen und die Reaktionszeit verringern.
10. Vor allem im letzten Fall (9) hatte der Angriff auf Israel auch Folgen für die Angreiferinnen und Angreifer selbst. Das Gebäude, von dem aus der Angriff stattgefunden hatte, wurde zerstört und der Angriff erfolgreich abgewehrt. Es handelte sich zwar um eine bisher einmalige Art und Weise einen Cyber-Angriff abzuwehren, die aber laut der Studie von [38] etwa 60% bis 65% der Bevölkerung befürworten würden (vergleiche mit Abbildung 7: Prozentuale Bevorzugung der Vergeltungsmaßnahmen [38]).

Die folgenden fünf Techniken bieten Ansätze dazu, wie sich der Erfolg auf Seiten der Angreiferin beziehungsweise des Angreifers reduzieren lässt. Die originalen Techniken von [81] lassen sich hier nur zum Teil im Cyber-Raum anwenden. Insbesondere das Markieren von Eigentum und Stören von Märkten ist nicht mit den Zielen von Cyber-Terrorismus vereinbar (vergleiche Straftaten nach österreichischem Gesetz [14]). Stattdessen wurden zwei neue Techniken eingeführt, welche sich auf Einschränkung des Angriffspotenzials und der Vermeidung von Schäden konzentrieren.

11. Ein Beispiel, wo das Verbergen von Zielen sinnvoll angewandt werden kann ist Fall 8 in der Ukraine. Die Angreifer konnten mithilfe eines Netzwerkscans andere Systeme, insbesondere den Active Directory Server, ausfindig machen und anschließend den eigentlichen Angriff fortsetzen. Der Einsatz entsprechender Werkzeuge, die eine Erkennung von anderen Geräten im Netzwerk erschweren beziehungsweise verhindern ist hier zielführend.

12. Eine Möglichkeit Ziele für den Cyber-Terroristen zu entfernen ist Services, die nicht zwingend eine Internetverbindung benötigen zu isolieren und sie damit für die Angreiferin oder den Angreifer unerreichbar zu machen. Dazu ist es nötig solche Systeme zu identifizieren und bei Bedarf auf andere Lösungen umzusteigen, wenn die bestehende Technologie das nicht erlaubt.
13. Wenn es der Angreiferin oder dem Angreifer so wie in Fall 8 schon gelingt die Zugangsdaten von Benutzern zu erlangen kann man hier entgegenwirken, indem man die Rechte einschränkt. Es ist zwar nicht klar, ob es sich in Fall 8 um einen Administratoraccount handelte, aber man hätte in diesem Fall Remotezugriffe unterbinden können beziehungsweise auch Remotezugriff auf Systeme generell verbieten können, wenn dies nicht erforderlich ist.
14. Wenn der Strom ausfällt, weil Umspannwerke nicht mehr funktionieren, wie in Fall 8 ist es schwer zu argumentieren, dass es einen alternativen Standort gibt. Anders ist das aber bei einer gestörten Mailkommunikation (Fall 1) oder einer überlasteten Telefonanlage (Fall 8). Durch den Einsatz alternativer Kommunikationswege kann der Erfolg der Terroristinnen und Terroristen verringert werden. Da in Fall 1 nur die Mailkommunikation beeinträchtigt wurde, kann man notfalls auf Telefone umsteigen und bei Fall 8 andere Meldewege für Störungen etablieren, wie zum Beispiel E-Mail oder andere webbasierte Lösungen.
15. Einige Angreiferinnen und Angreifer haben nicht nur Webseiten blockiert, sondern sie gänzlich verunstaltet. Dies passierte zum Beispiel in den Fällen 4 und 6. Welches Ziel die Angreiferinnen und Angreifer damit tatsächlich verfolgt haben ist nicht ganz sicher, aber durch Abschalten der betroffenen Seiten ist es nicht möglich die falschen Inhalte abzurufen.

Die letzten fünf Techniken wurden nur zum Teil von [81] übernommen. Es handelt sich dabei um die Techniken 19. Gruppenzwang neutralisieren und 20. Nachahmung vermieden. Die anderen drei Techniken wurden neu aus den 9 Fällen herausgearbeitet. Insgesamt setzen sie zunächst darauf, die Terroristinnen und Terroristen nicht zu provozieren überhaupt einen Angriff zu starten. Das heißt man muss die Radikalisierung und Unruhestiftung in der Bevölkerung vermeiden. Außerdem werden Techniken präsentiert, wie man einen Angriff vermeiden kann, wenn es fast schon zu spät ist und wie man Folgeangriffe meidet.

16. Viele der präsentierten Fälle von Cyber-Terrorismus sind mit Konflikten im realen Leben verbunden. Dies gilt zum Beispiel für Fall 1 (Konflikt mit Minderheit), Fall 3 (Konflikt Russland mit Estland), Fall 4 (Konflikt Russland mit Georgien), Fall 7 (Konflikt zwischen Nord- und Südkorea) und Fall 9 (Konflikt zwischen Hamas und Israel). Speziell in Fällen wie Estland führte das unbedachte Versetzen eines Monuments zu großen Unruhen innerhalb Estlands. Solche Spannungen sind vorab zu erkennen, um zusätzliche Provokationen zu vermeiden, die dann in Cyber-Angriffen enden.
17. In den Fällen 4 (Georgien) und 5 (Vereinigte Staaten) blieben spürbare Folgen teilweise oder ganzheitlich aus. In Georgien wurde zum Beispiel keine kritische Infrastruktur angegriffen, während in den Vereinigten Staaten ebenfalls keine Auswirkungen für die Bevölkerung spürbar wurden. An dieser Stelle ist es aber schwer zu sagen, was die Betreiberinnen und Betreiber in den beiden Fällen richtig gemacht haben, um nicht angegriffen zu werden. Offensichtlich muss es seitens der Angreiferinnen und Angreifer einen Grund gegeben haben die Ziele nicht anzugreifen. Auch wenn es nicht ganz klar ist, was dieses „richtige“ Verhalten war, zeigt es, dass gewisse Aktionen vorab überdacht werden sollten, wenn man schon im Visier der Terroristinnen und Terroristen ist und kurz vor einem Angriff steht.
18. Bei einigen komplexeren Angriffen, wie in der Ukraine (Fall 8) brauchte es etwas versiertere Angreiferinnen und Angreifer mit der nötigen Expertise. Daher sollte bereits von Anfang an verhindert werden, dass sich viele Personen dazu radikalisieren lassen. Um hier entgegen zu wirken, kann man zum Beispiel bekannte Foren von Terrorristinnen und Terroristen überwachen und die Betreiber der Seite dazu zwingen die Inhalte offline zu nehmen. In den Fällen 3 und 4 herrschte ein aktiver Austausch in Foren (zum Beispiel www.StopGeorgia.ru bei den Angriffen auf Georgien). Außerdem gibt es auf verschiedenen Social Media Plattformen Konten, die aktiv Werbung für terroristische Organisationen machen. An dieser Stelle muss weiter an der frühzeitigen Erkennung entsprechender Profile gearbeitet werden (siehe auch Kapitel 2.2 Cyber-Terrorismus in sozialen Netzwerken)
19. Durch Aufforderungen an russische Patriotinnen und Patrioten konnte man in Estland und teilweise auch Georgien viele Personen dazu animieren an den Angriffen teilzunehmen. Durch entsprechende Anleitungen wurde es noch einfacher die Massen zu mobilisieren. An dieser Stelle muss daran gearbeitet werden entsprechende Provokationen offline zu nehmen, damit sich möglichst wenige mögliche Angreiferinnen und Angreifer davon provozieren lassen.
20. Nachdem ein Fall von Cyber-Terrorismus bekannt geworden ist, ist es wichtig die gefundenen Angriffsmöglichkeiten zu beseitigen. Einige Angriffe starteten mit Phishing Mails, andere zielten auf

einen Denial of Service ab. Wenn nachträglich keine Verbesserung der Defensivmaßnahmen in Kraft tritt, kann es aufgrund der publizierten Details zum Angriff leichter sein, den gleichen Angriff nochmals auszuführen. Eine derartige Nachahmung lässt sich nur vermeiden, wenn man die Awareness der Mitarbeiterinnen und Mitarbeiter erhöht und Softwareschwachstellen beseitigt. Zusätzlich muss man die Erkennung von Malware verbessern, wenn dies Teil des Angriffs war, um nicht derselben Schadsoftware ein zweites Mal zum Opfer zu fallen. Eine Geheimhaltung der Informationen zum Angriff ist nicht zielführend, da somit keine Details zu neuer Schadsoftware publik werden und hier nicht nachgebessert werden kann. Außerdem blieben Schwachstellen der Öffentlichkeit unbekannt und somit wären andere potenzielle Ziele im Nachteil, da sie entsprechende Lücken nicht kennen und schließen können.

In den aufgearbeiteten neun Fällen gibt es sehr viele Informationen darüber, wie die Angreiferinnen und Angreifer vorgegangen sind. Teilweise gab es Bekenntnisse zu den Fällen, wie in Estland (Fall 3) und Saudi-Arabien (Fall 6). Was aber oftmals ausbleibt sind Konsequenzen für die Täter. Diese bleiben in Estland weitestgehend aus und auch in Saudi-Arabien wurden nicht alle Angreiferinnen und Angreifer verurteilt. Dies ist aber oftmals auf fehlende Spuren zu zurückzuführen. Entschuldigungen zu vermeiden führt daher zwangsläufig zu dem Problem, dass die Terroristen trotz der gefundenen Beweise nicht immer zur Rechenschaft gezogen werden können, weil es nicht sicher bewiesen werden konnte. Aus diesem Grund führt diese Kategorie auf den Cyber-Raum übertragen auf Technik Nummer neun zurück, dass die Anonymität verringert werden muss.

Erhöhen des Aufwands	**Erhöhen der Risiken**	**Verringern des Erfolgs**	**Provokation verringern**
1. Hardening: ■ Server und Infrastruktur ■ Überprüfung von Mitarbeitern und Partnern	*6. Zusammenarbeit:* ■ Informationen teilen ■ Analyse von Experten	*11. Ziele verbergen:* ■ „Verstecken“ von Geräten im Netzwerk	*16. Vermeiden von Eskalationen:* ■ Erkennen von Konflikten
2. Servicezugriffe: ■ Multifaktor-Authentifizierung	*7. Automatisierte Überwachung:* ■ Verfolgung von Angreifern mittels Tracking-Tools	*12. Ziele entfernen:* ■ Verbindung zum Internet trennen, falls möglich	*17. Keinen Grund zum Angriff geben:* ■ „Richtiges“ Verhalten aus Sicht des Ziels
3. Ausgänge prüfen (nur physisch): ■ Durchsuchen von Personen	*8. Manuelle Überwachung:* ■ Auditieren von Logs ■ Belohnungen für Meldungen	*13. Reduzieren des Potenzials:* ■ Nur nötige Nutzerrechte vergeben ■ Zugriffsmöglichkeiten reduzieren	*18. Radikalisierung vermeiden:* ■ Foren überwachen ■ Social Media kontrollieren
4. Servicetrennung: ■ Physische Trennung von unabhängigen Services	*9. Anonymität verringern:* ■ Registrierung mit eindeutiger Identifikation einfordern	*14. Alternativen bei Ausfällen:* ■ Mehrere Wege zur Verständigung und Koordination	*19. Gruppenzwang neutralisieren:* ■ Öffentliche Kundmachungen offline nehmen
5. Werkzeuge kontrollieren: ■ Internetzugänge verbieten ■ Internetfähige Geräte nicht verkaufen	*10. Abwehr des Angriffs:* ■ Schäden beim Angreifer selbst verursachen.	*15. Vorteile verweigern:* ■ Abschalten verunstalteter Webseiten	*20. Nachahmung verhindern:* ■ Patchen von Systemen ■ Erkennung von Malware verbessern ■ Beseitigen der Schwachstellen

Tabelle 22: Techniken zur Vermeidung von Cyber-Terrorismus

6. Zusammenfassung

In dieser Arbeit wurden neun Fälle von Cyber-Terrorismus zwischen 1998 und 2019 genauer untersucht und einige Aspekte zu jedem Fall beschrieben. Dadurch entstand ein Überblick über die wesentlichsten Fälle von Cyber-Terrorismus in den vergangenen Jahren. Insgesamt betrachtet hat Cyber-Terrorismus noch nicht die Dimensionen von herkömmlichem Terrorismus erreicht, da großangelegte Angriffe, die mit den Anschlägen vom 11. September 2001 vergleichbar wären, noch nicht stattgefunden haben. Auch wenn die Schäden bis jetzt noch nicht derartige Höhen erreicht haben, ist nicht auszuschließen, dass Cyber-Terroristen zukünftig für vergleichbare Fälle sorgen. In jedem Fall ist klar festzustellen, dass Terroristen das Internet bereits heute zu verschiedensten Zwecken nutzen und voraussichtlich in Zukunft auch noch nutzen werden.

In den betrachteten neun Fällen wurde näher auf die terroristischen Angreifer, deren Ziele, Vorgehensweise und die Folgen der Angriffe eingegangen. Durch den Vergleich der Fälle untereinander konnten zusätzlich Parallelen erkannt werden, die hinsichtlich der betrachteten Aspekte zu den Fällen existieren. Unternehmen können dadurch anhand ihrer eigenen Charakteristiken genauer analysieren, wie groß ihr eigenes Bedrohungspotenzial für Cyber-Terrorismus ist.

Da mithilfe von Frameworks, wie STIX, zukünftig ein besserer Informationsaustausch zu Fällen von Cyber-Terrorismus durchgeführt werden kann, wurden beispielhaft zwei der neun Fälle in STIX beschrieben. Im Zuge dessen ließen sich die wesentlichsten Merkmale der beiden Cyber-Terror-Fälle beschreiben. STIX bietet durch die vorgegebenen Elemente einen Rahmen, welche Eigenschaften bei einem cyber-terroristischen Angriff betrachtet werden sollten. Durch das maschinenlesbare Format von STIX ist der einfache und schnelle Informationsaustausch inklusive Analyse möglich. Außerdem ist es nicht mehr nötig eine händische Analyse bei jedem Fall durchzuführen. Insbesondere dadurch können viele Informationen sehr schnell erfasst und verarbeitet werden. Zukünftig könnte das einen Vorteil in der Dokumentation eines terroristischen Cyber-Angriffs bringen, da man besser weiß welche Einzelheiten genauer dokumentiert werden müssen. Dies könnte ein Ziel weiterer Forschungen sein.

Schließlich konnten 20 Techniken herausgearbeitet werden, um Großteiles präventive Maßnahmen gegen Cyber-Terroristinnen und Cyber-Terroristen zu setzen. Diese Techniken können von Unternehmen und Regierungen eingesetzt werden, um vorab dafür zu sorgen nicht ins Visier von Cyber-Terroristinnen und Cyber-Terroristen zu geraten beziehungsweise Schäden und andere negative Folgen zu verringern.

In dieser Arbeit wurden nur einige ausgewählte Fälle von Cyber-Terrorismus behandelt, keinesfalls aber alle weltweit existierenden Fälle. Einerseits ist das darauf zurückzuführen, dass es noch keine anerkannte Definition dafür gibt, was alles unter den Begriff von Cyber-Terrorismus fällt. Zukünftige Arbeiten können an dieser Stelle weiter ansetzen, um diesen Begriff von verwandten Themen, wie Hacktivismus oder Cyber-Warfare, abgrenzen zu können. Andererseits ist eine verständliche Verschwiegenheit seitens der Opfer von Cyber-Terrorismus zu erkennen, da zum Teil veröffentlichte Informationen den Angreifern einen Vorteil verschaffen könnten. Um Cyber-Terroristen zukünftig besser identifizieren und nachverfolgen zu können, kann eine Zusammenarbeit mit Experten und eine Veröffentlichung von Informationen aber helfen. Es wäre daher sinnvoll in dieser Richtung nach Lösungen zu suchen, die beide Interessen abdecken.

Literaturverzeichnis

[1] L. Rabe, „Statistiken zur Internetnutzung weltweit," Statista, 21 Juni 2019. [Online]. Available: https://de.statista.com/themen/42/internet/. [Zugriff am 13 Juli 2019].

[2] M. Brandt, „Twitter hat bislang 936.000 Terror-Profile gesperrt," Statista, 20 September 2017. [Online]. Available: https://de.statista.com/infografik/11165/durch-twitter-gesperrte-profile-mit-terrorbezug/. [Zugriff am 13 Juli 2019].

[3] Statista, „Anzahl der aufgrund von Terrorverdacht entfernten Inhalte auf Facebook weltweit vom 1. Quartal 2018 bis zum 1. Quartal 2019 (in Millionen)," Statista, 27 Mai 2019. [Online]. Available: https://de.statista.com/statistik/daten/studie/942982/umfrage/anzahl-der-aufgrund-von-terrorverdacht-entfernten-inhalte-auf-facebook-weltweit/. [Zugriff am 13 Juli 2019].

[4] F. Tenzer, „Anteil der Unternehmen mit Internetzugang in europäischen Ländern im Jahr 2018," Statista, 2018. [Online]. Available: https://de.statista.com/statistik/daten/studie/75574/umfrage/unternehmen-mit-internetzugang-in-der-eu/. [Zugriff am 13 Juli 2019].

[5] E. Schultz, „Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2018," Statista, 5 Juni 2019. [Online]. Available: https://de.statista.com/statistik/daten/studie/294141/umfrage/cybercrime-in-oesterreich/. [Zugriff am 13 Juli 2019].

[6] Statista, „Welche der folgenden Risiken bereiten Ihnen Sorgen?," Statista, 2015. [Online]. Available: https://de.statista.com/statistik/daten/studie/317484/umfrage/umfrage-zu-risikoempfinden-und-sorgen-der-oesterreicher/. [Zugriff am 13 Juli 2019].

[7] Europäische Union, „BESCHLUSS (GASP) 2019/25 DES RATES," Europäische Union, 9 Januar 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/de/TXT/HTML/?uri=CELEX:32019D0025&from=EN. [Zugriff am 8 Juli 2019].

[8] Außenministerium der Vereinigten Staaten von Amerika, „Foreign Terrorist Organizations," Außenministerium der Vereinigten Staaten von Amerika, 2019. [Online]. Available: https://www.state.gov/foreign-terrorist-organizations/. [Zugriff am 8 Juli 2019].

[9] M. Janson, „Opfer des Terrors," Statista, 20 September 2018. [Online]. Available: https://de.statista.com/infografik/15520/weltweite-opfer-von-terroranschlaegen/. [Zugriff am 13 Juli 2019].

[10] Duden, „Cyber," Duden, 2019. [Online]. Available: https://www.duden.de/suchen/dudenonline/Cyber. [Zugriff am 10 Juni 2019].

[11] S. Schumacher, „Cyber-Terrorismus – Reale Bedrohung oder Mythos?," in *Jahrbuch Terrorismus 2013/2014*, Verlag Barbara Budrich, 2014, pp. 159-178.

[12] W. Gibbson, Burning Chrome, Kanada: Omni, 1982.

[13] Duden, „Terror," Duden, 2019. [Online]. Available: https://www.duden.de/rechtschreibung/Terror#Bedeutung-1. [Zugriff am 10 Juni 2019].

[14] Bundesministerium für Digitalisierung und Wirtschaftsstandort, „§278c Terroristische Straftaten," Bundesministerium für Digitalisierung und Wirtschaftsstandort, 9 Juni 2019. [Online]. Available: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=0afd77ab-aa7b-4bb2-985c-f27b082f102e&Position=1&Abfrage=Bundesnormen&Gesetzesnummer=&VonParagraf=278c&FassungVom=09.06.2019&Dokumentnummer=NOR40208392. [Zugriff am 9 Juni 2019].

[15] D. E.-C. Meier, A. Hannemann und R. Meyer zum Felde, Wörterbuch zur Sicherheitspolitik: Deutschland in einem veränderten internationalen Umfeld, E.S. Mittler & Sohn GmbH, 2012.

[16] E. Luiijf, „Definitions of Cyber Terrorism," in *Cyber crime and cyber terrorism investigator's handbook*, Syngress, 2014, pp. 11-17.

[17] M. M. Pollitt, Cyberterrorism - fact or fancy?, Elsevier, 1998.

[18] D. E. Denning, „Cyberterrorism - Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of representatives," in *Focus on Terrorism, Band 9*, Nova Publishers, 2007, pp. 71-76.

[19] J. A. Lewis, Assessing the risks of cyber terrorism, cyber war and other cyber threats, Washington DC: Steptoe, 2002.

[20] M. Kenney, Cyber-Terrorism in a Post-Stuxnet World, Elsevier, 2015.

[21] Duden, „Krieg," Duden, 2019. [Online]. Available: https://www.duden.de/rechtschreibung/Krieg. [Zugriff am 10 Juli 2019].

[22] M. Robinsona, K. Jonesb und H. Janickea, Cyber Warfare: Issues and Challenges, Computers & Security, 2015.

[23] W. Füllgraf, Hacktivisten, Bundeskriminalamt (Deutschland), 2016.

[24] G. Weimann und J. Jost, Neuer Terrorismus und Neue Medien, Springer, 2015.

[25] R. Heickerö, „Cyber Terrorism: Electronic Jihad," in *Strategic Analysis Vol.38 Nr. 4*, Tylor & Francis, 2014, pp. 554-565.

[26] N. Ayres, L. A. Maglaras, H. Janicke, R. Smisth und Y. He, The mimetic virus: A vector for cyber terrorism, International Journal of Business Continuity and Risk Management, 2016.

[27] S. S. Sin, L. A. Blackerby, E. Asiamah und R. Washburn, Determining extremist organisations' likelihood of conducting cyber attacks, 8th International Conference on Cyber Conflict (CyCon): IEEE, 2016.

[28] G. Weimann, Terror on the Internet: The new arena, the new challenges, US Institute of Peace Press, 2006.

[29] G. Weimann, „Going Dark: Terrorism on the Dark Web," in *Studies in Conflict & Terrorism*, Taylor & Francis, 2016, pp. 195-206.

[30] Deep Web, „Deep Web Sites 2019 Dark Web Deep Web Links Hidden Wiki," Deep Web, 2019. [Online]. Available: https://www.deepweb-sites.com/. [Zugriff am 21 August 2019].

[31] Tor Project, „Tor Project," Tor Project, 2019. [Online]. Available: https://www.torproject.org/. [Zugriff am 21 August 2019].

[32] E. Dilipraj, „Terror in the Deep and Dark Web," in *Air Power Journal*, Air Power Journal, 2014, pp. 120-140.

[33] Kaggle Inc., „How ISIS Uses Twitter," Kaggle Inc., 2016. [Online]. Available: https://www.kaggle.com/fifthtribe/how-isis-uses-twitter. [Zugriff am 13 August 2019].

[34] Kaggle Inc., „Tweets Targeting Isis," Kaggle Inc., 2016. [Online]. Available: https://www.kaggle.com/activegalaxy/isis-related-tweets. [Zugriff am 13 August 2019].

[35] Z. Yunos, R. Ahmad, S. M. Ali und S. Shamsuddin, „Illicit activities and terrorism in cyberspace: an exploratory study in the southeast asian region," in *Pacific-Asia Workshop on Intelligence and Security Informatics*, Springer, 2012, pp. 27-35.

[36] S. Ruhil, „10 deadly terrorist groups on the planet," India Today, 27 November 2015. [Online]. Available: https://www.indiatoday.in/magazine/glossary/story/20151207-10-deadly-terrorist-groups-on-the-planet-820877-2015-11-25. [Zugriff am 5 Oktober 2019].

[37] I. Awan, Cyber-Extremism: Isis and the Power of Social Media, Springer, 2017.

[38] M. L. Gross, D. Canetti und D. R. Vashdi, The psychological effects of cyber terrorism, PubMed Central, 2016.

[39] S. Christoph, Funktionslogik terroristischer Propaganda im bewegten Bild, Journal for Deradicalization, 2015.

[40] R. Simon, Informationen, die Bilder haben. Zur Moderierbarkeit von visuellem Content, mediarep, 2018.

[41] V. N. Uzel, E. S. Eşsiz und S. A. Özel, Using Fuzzy Sets for Detecting Cyber Terrorism and Extremism in the Text, IEEE, 2018.

[42] M. Munezero, M. Mozgovoy, T. Kakkonen, V. Klyuev und E. Sutinen, Antisocial Behavior Corpus for Harmful Language Detection, IEEE, 2013.

[43] A. L. Maas, R. E. Daly, P. T. Pham, D. Huang, A. Y. Ng und C. Potts, „Learning Word Vectors for Sentiment Analysis," in *Proceedings of the 49th Annual Meeting of the Association for Computational Linguistics: Human Language Technologies*, Portland, Oregon, USA, Association for Computational Linguistics, 2011, pp. 142-150.

[44] M. Fernandez, M. Asif und A. Harith, „Understanding the Roots of Radicalisation on Twitter," in *WebSci'18 Proceedings of the 10th ACM Conference on Web Science*, Amsterdam, ACM, 2018, pp. 1-10.

[45] J. M. Berger und J. Morgan, The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter., The Brookings Institution, 2015.

[46] R. Lara-Cabrera, A. Gonzalez-Pardo und D. Camacho, Statistical analysis of risk assessment factors and metrics to evaluate radicalisation in Twitter, Elsevier, 2017.

[47] M. Rowe und H. Saif, Mining pro-ISIS radicalisation signals from social media users, Tenth International AAAI Conference on Web and Social Media, 2016.

[48] M. Vergani und A.-M. Bliuc, The evolution of the ISIS'language: a quantitative analysis of the language of the first year of Dabiq magazine, Sicurezza, Terrorismo e Società= Security, Terrorism and Society, 2015.

[49] B. G. Gomes, P. H. Holanda, A. P. Couto da Silva und O. Goussevskaia, „Profiling ISIS Supporters on Twitter," in *Proceedings of the 23rd Brazillian Symposium on Multimedia and the Web*, ACM, 2017, pp. 457-460.

[50] F. M. Moghaddam, „The staircase to terrorism: A psychological exploration," in *American Psychologist*, American Psychological Association, 2005, pp. 161-169.

[51] J. Victoroff, „The mind of the terrorist: A review and critique of psychological approaches," in *Journal of Conflict resolution*, Sage Publications, 2005, pp. 3-42.

[52] M. J. Charvat, „Cyber Terrorism: A New Dimension in Battlespace," in *The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, 2009, pp. 77-87.

[53] B. Krebs, „Terrorism's Hook Into Your Inbox," The Washington Post, 5 Juli 2007. [Online]. Available: https://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501153.html??noredirect=on. [Zugriff am 11 August 2019].

[54] M. Jacobson, Terrorist Financing and the Internet, Routledge, 2010.

[55] D. Maurice, New Threats and Countermeasures in Digital Crime and Cyber Terrorism, IGI Global, 2015.

[56] K. A. Paul, Ancient Artifacts vs. Digital Artifacts: New Tools for Unmasking the Sale of Illicit Antiquities on the Dark Web, MDPI, 2018.

[57] T. K. Marion G. Müller, Terror der Bilder, Springer, 2019.

[58] B. M. Jenkins, Will terrorists go nuclear?, Santa Monica: Rand Corporation, 1975.

[59] J. S. Lerner, R. M. Gonzalez, D. A. Small und B. Fischhoff, „Effects of fear and anger on perceived risks of terrorism: A national field experiment," in *Psychological science*, Los Angeles, SAGE Publications, 2003, pp. 144-150.

[60] Laenderdaten.info, „Die größten Terrorgruppen im Vergleich," Laenderdaten.info, 2017. [Online]. Available: https://www.laenderdaten.info/terrorismus/terrorgruppen.php. [Zugriff am 14 August 2019].

[61] J. Rudnicka, „Entwicklung der Weltbevölkerungszahl von Christi Geburt bis zum Jahr 2020 (in Milliarden)," Statista, 13 August 2019. [Online]. Available: https://de.statista.com/statistik/daten/studie/1694/umfrage/entwicklung-der-weltbevoelkerungszahl/. [Zugriff am 14 August 2019].

[62] Statista, „Gefallene Soldaten im Ersten Weltkrieg nach Ländern in den Jahren 1914 bis 1918 (in 1.000 Personen)," Statista, 14 Juni 2008. [Online]. Available: https://de.statista.com/statistik/daten/studie/251868/umfrage/militaerische-verluste-im-ersten-weltkrieg-1914-bis-1918/. [Zugriff am 14 August 2019].

[63] V. Wagener, „Erinnerungen an einen Tag im Mai," Deutsche Welle, 8 Mai 2015. [Online]. Available: https://www.dw.com/de/erinnerungen-an-einen-tag-im-mai/a-18416664. [Zugriff am 14 August 2019].

[64] J. Hua und S. Bapna, „How can we deter cyber terrorism?," in *Information Security Journal: A Global Perspective*, Taylor & Francis, 2012, pp. 102-114.

[65] C. Spielberger, R. Gorsuch und R. Lushene, Manual for the State-Trait Anxiety Inventory, Palo Alto: Consulting Psychologists Press, 1970.

[66] M. W. David und S. Kouichi, Combating cyber terrorism: countering cyber terrorist advantages of surprise and anonymity, IEEE, 2003.

[67] RED-Alert, „RED-Alert," RED-Alert, 2019. [Online]. Available: http://redalertproject.eu/. [Zugriff am 8 August 2019].

[68] M. Fischer und R. Pelzer, Die Logik des Anschlags, Campus Verlag, 2016.

[69] R. von Solms und J. van Niekerk, „From information security to cyber security," in *Cybercrime in the Digital Economy*, Südafrika, Elsevier, 2013, pp. 97-102.

[70] M. Albahar, Cyber Attacks and Terrorism: A Twenty-First Century Conundrum, Science and engineering ethics: Springer, 2017.

[71] G. Jervas, Terrorismens tid, SNS Förlag, 2003.

[72] R. Langner, Stuxnet: Dissecting a Cyberwarfare Weapon, IEEE, 2011.

[73] W. A. Owens, K. W. Dam und H. S. Lin, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, IEEE Security and Privacy: Computer Science and Telecommunications Board, 2009.

[74] P. Vats, A comprehensive review of Cyber Terrorism in the current scenario, IEEE, 2016.

[75] Duden, „Kriminologie," Duden, 2019. [Online]. Available: https://www.duden.de/rechtschreibung/Kriminologie. [Zugriff am 19 August 2019].

[76] D. B. Parker, Computer Security Management, Reston Publishing Company Reston, VA, 1981.

[77] R. Willison, Understanding the perpetration of employee computer crime in the organisational context, Elsevier, 2006.

[78] A. Chalfin und J. McCrary, Criminal deterrence: A review of the literature, Journal of Economic Literature, 2017, pp. 5-48.

[79] A. Greenberg, „Hackers Remotely Kill a Jeep on the Highway - With Me in It," Wired, 21 Juli 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Zugriff am 30 Oktober 2019].

[80] R. Luh, Six Ways to Kill by Hacking, St. Pölten, 2013.

[81] D. B. Cornish und R. V. Clarke, „Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention," in *Crime prevention studies*, Bd. 16, Criminal Justice Press, 2003, pp. 41-96.

[82] D. B. Cornish, „The procedural analysis of offending and its relevance for situational prevention," in *Crime prevention studies*, Bd. 3, New York, Criminal Justice Press Monsey, 1994, pp. 151-196.

[83] Audit Commission for Local Authorities in England and Wales, Ghost in the machine: an analysis of IT fraud and abuse, Audit Commission, 1998.

[84] T. L. Friedman, The Lexus and the Olive Tree, Farrar, Straus and Giroux, 2000, p. 383.

[85] L. Rocci, Ethical Impact of Technological Advancements and Applications in Society, IGI Global, 2012, p. 267.

[86] S. Daly, J. Parachini und W. Rosenau, Aum Shinrikyo, Al Qaeda, and the Kinshasa Reactor, Santa Monica Kalifornien: RAND Corproration, 2005.

[87] R. Ottis, „Analysis of the 2007 cyber attacks against estonia from the information warfare perspective," in *Proceedings of the 7th European Conference on Information Warfare*, Academic Conferences Limited, 2008, pp. 163-168.

[88] S. Herzog, Revisiting the Estonian cyber attacks: Digital threats and multinational responses., Journal of Strategic Security, 2011, pp. 49-60.

[89] D. Hollis, Cyberwar Case Study: Georgia 2008, Small Wars Foundation, 2011.

[90] C. Berlich, „Der russisch-georgische Krieg 2008," in *Was ist dran am Cyber-Krieg? Eine Analyse moderner Kriegsführung am Beispiel des russisch-georgischen Krieges 2008*, disserta Verlag, 2016, pp. 54-74.

[91] S. Gorman, „Electricity grid in US penetrated by spies," The Wall Street Journal, 8 April 2009. [Online]. Available: https://www.wsj.com/articles/SB123914805204099085. [Zugriff am 13 Januar 2020].

[92] British Broadcasting Corporation, „South Korea network attack 'a computer virus'," British Broadcasting Corporation, 20 März 2013. [Online]. Available: https://www.bbc.com/news/world-asia-21855051. [Zugriff am 12 Dezember 2019].

[93] Hewlett Packard, Profiling an enigma: The mystery of North Korea's cyber threat landscape, Bd. 16, Hewlett Packard, 2014.

[94] Syrian Electronic Army, „Saudi Arabia Provinces Websites Hacked," Syrian Electronic Army, 2014. [Online]. Available: https://web.archive.org/web/20140321062345/http://sea.sy/article/id/2027/en. [Zugriff am 3 Januar 2020].

[95] D. Neal, „Syrian Electronic Army attacks Saudi websites," Business Media, 16 Januar 2014. [Online]. Available: https://www.theinquirer.net/inquirer/news/2323371/syrian-electronic-army-attacks-saudi-websites. [Zugriff am 3 Januar 2020].

[96] US Department of Homeland Security CISA Cyber + Infrastructure, „Cyber-Attack Against Ukrainian Critical Infrastructure," US Department of Homeland Security CISA Cyber + Infrastructure, 25 Februar 2016. [Online]. Available: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01. [Zugriff am 19 November 2019].

[97] Міністерство енергетики та вугільної промисловості України, „Продовжено роботу групи з вивчення причин тимчасового збою в роботі систем енергопостачальних компаній, що мали місце 23 грудня 2015 року," Міністерство енергетики та вугільної промисловості України, 20 Januar 2016. [Online]. Available: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245082298&cat_id=35109. [Zugriff am 21 November 2019].

[98] J. A. Gross, „IDF says it thwarted a Hamas cyber attack during weekend battle," The Times of Israel, 5 Mai 2019. [Online]. Available: https://www.timesofisrael.com/idf-says-it-thwarted-a-hamas-cyber-attack-during-weekend-battle/. [Zugriff am 9 Dezember 2019].

[99] S. Muttukrishna, Terrorism'or 'Liberation'? Towards a Distinction: A Case Study of the Armed Struggle of the Liberation Tigers of Tamil Eelam (LTTE)., SSRN, 2018.

[100] S. Ganguly, Ending the Sri Lankan Civil War, Dædalus, 2018.

[101] V. Golovnin, „Aum Cult Implicated in Nuclear Information Stealing," Itar-Tass News Agency, 29 März 2000. [Online]. Available: https://fas.org/sgp/news/2000/03/aum.html. [Zugriff am 2 Dezember 2019].

[102] Nuclear Threat Initiative, „Aum Shinrikyo Alleged to Have Obtained Data on Russian, Ukrainian Nuclear Power Plants," Nuclear Threat Initiative, 27 März 2000. [Online]. Available: https://www.nti.org/analysis/articles/aum-shinrikyo-alleged-have-obtained-data-russian-ukrainian-nuclear-power-plants/. [Zugriff am 2 Dezember 2019].

[103] Monterey Institute of International Studies, „Chronology of Aum Shinrikyo's CBW Activities," Monterey Institute of International Studies, 2001. [Online]. Available: https://www.nonproliferation.org/wp-content/uploads/2016/06/aum_chrn.pdf. [Zugriff am 2 Dezember 2019].

[104] Kamigraphie Wiki-Projekt der Universität Wien, „Asahara Shōkō," Universität Wien, 4 September 2018. [Online]. Available: https://www.univie.ac.at/rel_jap/kami/Asahara_Sh%C5%8Dk%C5%8D. [Zugriff am 2 Dezember 2019].

[105] A. Bazhova, „Russian Ministry Denies Aum Shinrikyo Had Access to Data," Itar-Tass News Agency, 29 März 2000. [Online]. Available: https://fas.org/sgp/news/2000/03/aum.html. [Zugriff am 2 Dezember 2019].

[106] Japan Times Ltd., „Sumitomo Bank, Hosei University on Aum-related PC firms' client list," Japan Times Ltd., 12 März 2000. [Online]. Available: https://www.japantimes.co.jp/news/2000/03/12/national/sumitomo-bank-hosei-university-on-aum-related-pc-firms-client-list/#.XeZRMOhKiUl. [Zugriff am 3 Dezember 2019].

[107] A. Bright, Estonia accuses Russia of 'cyberattack', Christian Science Monitor, 2007.

[108] M. Ehala, „The Bronze Soldier: Identity Threat and Maintenance in Estoni," in *From Post-Communism to the EU: Estonia's Transition 20 Years on*, Journal of Baltic Studies, Routledge, 2009, pp. 139-158.

[109] M. D. Cavelty, „Critical information infrastructure: vulnerabilities, threats and responses," in *Disarmament Forum*, 2007, 2007, pp. 15-22.

[110] Urban Dictionary, „Pidor," Urban Dictionary, 21 März 2009. [Online]. Available: https://www.urbandictionary.com/define.php?term=pidor. [Zugriff am 22 Oktober 2019].

[111] British Broadcasting Corporation, „The cyber raiders hitting Estonia," British Broadcasting Corporation, 17 Mai 2007. [Online]. Available: http://news.bbc.co.uk/2/hi/europe/6665195.stm. [Zugriff am 23 Oktober 2019].

[112] F. Delerue, „Attribution to State of Cyber Operations Conducted by Non-State Actors," in *Use and Misuse of New Technologies*, Springer, 2019, pp. 233-255.

[113] C. Clover, „Kremlin-backed group behind Estonia cyber blitz," *Financial Times UK,* p. 8, 11 März 2009.

[114] M. De Wulf, „Bevölkerung Russlands 2007," PopulationPyramid.net, 2007. [Online]. Available: https://www.populationpyramid.net/de/russland/2007/. [Zugriff am 22 Oktober 2019].

[115] R. Heller, „Die Russische Jugendbewegung "Naschi". Aufstieg Und Fall Eines Polittechnologischen Projekts in der Era Putin," in *Russland-Analysen*, Länder-Analysen, 2008, pp. 2-6.

[116] INSEAD; The World Economic Forum, „Global Information Technology Report 2006 - 2007," INSEAD; The World Economic Forum, 27 März 2007. [Online]. Available: https://www.insead.edu/news/2007-WE-forum-release. [Zugriff am 23 Oktober 2019].

[117] K. Ruus, E-stonia: Pioneer of Internet Innovation and E-Government, European Affairs, 2007.

[118] T. Eneken, K. Kadri und V. Liis, International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010.

[119] C. Wilson, Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress, LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, 2008.

[120] T. TARK, Die Mobilisierungen des Jahres 1944 in Estland: Ein Triumph der deutschen Propaganda?, Forschungen zur Baltischen Geschichte, 2014.

[121] T. Randel, „CERT Eesti tegevuse aastakokkuvõte 2007," Estonian Informatics Centre, 2007.

[122] C. Rhoads, Cyber Attack Vexes Estonia, The Wall Street Journal, 2007.

[123] K. Ruus, Cyber war I: Estonia attacked from Russia, Columbia International Affairs Online, 2008.

[124] M. Lehti, M. Jutila und M. Jokisipilä, „Never-ending Second World War: Public performances of national dignity and the drama of the Bronze soldier," in *Journal of Baltic Studies*, 4 Hrsg., Bd. 39, Taylor & Francis, 2008, pp. 393-418.

[125] N. Schachtman, „Top Georgian Official: Moscow Cyber Attacked Us - We Just Can't Prove It," Wired, 11 März 2009. [Online]. Available: https://www.wired.com/2009/03/georgia-blames/. [Zugriff am 27 Dezember 2019].

[126] J. Carr, Russia/Georgia Cyber War - Findings and Analysis, Project Grey Goose, 2008.

[127] J. Bumgarner und S. Borg, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, United States Cyber Consequences Unit, 2009.

[128] StopGeorgia.ru, „Первоочередные цели для атак (Die Hauptziele für Angriffe sind)," StopGeorgia.ru, August 2008. [Online]. Available: https://web.archive.org/web/20080812084132/http://www.stopgeorgia.ru/?pg=tar. [Zugriff am 28 Dezember 2019].

[129] H. Jahankhani, A. G. Hessami und F. Hsu, „Situation, along the conflict, of the websites listed as preferential targets," in *Global Security, Safety, and Sustainability*, Springer, 2009, pp. 38-40.

[130] G. Keizer, „Russian hacker 'militia' mobilizes to attack Georgia," Network World, 12 August 2008. [Online]. Available: https://web.archive.org/web/20150816133606/http://www.networkworld.com/article/2274800/lan-wan/russian-hacker--militia--mobilizes-to-attack-georgia.html. [Zugriff am 30 Dezember 2019].

[131] R. J. Deibert, R. Rohozinski und M. Crete-Nishihata, Cyclones in cyberspace: Information shaping and denial in the 2008 Russia--Georgia war, London: Sage Publications, 2012.

[132] J. Meserve, „Hackers reportedly have embedded code in power grid," Cable News Network, 9 April 2009. [Online]. Available: http://edition.cnn.com/2009/TECH/04/08/grid.threat/index.html. [Zugriff am 13 Januar 2020].

[133] History.com, „Blackout hits Northeast United States," History.com, 14 August 2019. [Online]. Available: https://www.history.com/this-day-in-history/blackout-hits-northeast-united-states. [Zugriff am 13 Januar 2020].

[134] J. van der Wel, Cyber Tactics in the Syrian Civil War: An Analysis of the Syrian Electronic Army, Niederlande: Leiden University, 2018.

[135] E. Kovacs, „16 Saudi Arabian Government Websites Hacked by Syrian Electronic Army," Softpedia, 16 Januar 2014. [Online]. Available: https://news.softpedia.com/news/16-Saudi-Arabian-Government-Websites-Hacked-by-Syrian-Electronic-Army-417751.shtml#sgal_0. [Zugriff am 3 Januar 2020].

[136] Syrian Electronic Army, „Meet the SEA Team/SEA Story," Syrian Electronic Army, 13 März 2014. [Online]. Available: https://web.archive.org/web/20140313033618/http://sea.sy:80/index/en. [Zugriff am 3 Januar 2020].

[137] L. Murphy, „Anonymous isn't ready to publish the identities of the Syrian Electronic Army-yet," The Daily Dot, 5 September 2013. [Online]. Available: https://www.dailydot.com/news/anonymous-syrian-electronic-army-names/. [Zugriff am 3 Januar 2020].

[138] US Department of Justice, „Two Members of Syrian Electronic Army Indicted for Conspiracy," US Department of Justice, 17 Mai 2018. [Online]. Available: https://www.justice.gov/usao-edva/pr/two-members-syrian-electronic-army-indicted-conspiracy. [Zugriff am 3 Januar 2020].

[139] M. Baezner und P. Robin, The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict, Zürich: Eidgenössische Technische Hochschule Zürich, 2017.

[140] E. Lockley und B. Akhgar, „Understanding the situational awareness in cybercrimes," in *Cyber crime and cyber terrorism investigator's handbook*, Syngress, 2014, pp. 101-121.

[141] British Broadcasting Corporation, „China IP address link to South Korea cyber-attack," British Broadcasting Corporation, 21 März 2013. [Online]. Available: https://www.bbc.com/news/world-asia-21873017. [Zugriff am 16 Dezember 2019].

[142] British Broadcasting Corporation, „South Korea says China hack link a 'mistake'," British Broadcasting Corporation, 22 März 2013. [Online]. Available: https://www.bbc.com/news/world-asia-21891617. [Zugriff am 16 Dezember 2019].

[143] R. Sherstobitoff, I. Liba und J. Walter, Dissecting Operation Troy: Cyberespionage in South Korea, Korea: McAfee, 2013.

[144] Associated Press, „North Korea launched cyber attacks, says south," 11 Juli 2009. [Online]. Available: https://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks. [Zugriff am 18 Dezember 2019].

[145] L. Se Young, „UPDATE 2-S.Korea network hack prompts broadcast, bank outages," CNBC, 20 März 2013. [Online]. Available: https://web.archive.org/web/20130330172233/http://www.cnbc.com/id/100571450. [Zugriff am 16 Dezember 2019].

[146] Finance.ua, „Хакери атакували «Прикарпаттяобленерго», знеструмивши половину регіону на 6 годин (Hacker griffen Prykarpattyaoblenergo an und zerschmetterten 6 Stunden lang die Hälfte der Region)," Finance.ua, 25 Dezember 2015. [Online]. Available: https://news.finance.ua/ua/news/-/366136/hakery-atakuvaly-prykarpattyaoblenergo-znestrumyvshy-polovynu-regionu-na-6-godyn. [Zugriff am 19 November 2019].

[147] M. Gonchar, „The Impact of Russian Aggression Against Ukraine on CEI," in *Addressing Emerging Security Risks for Energy Networks in South Caucasus*, Bd. 137, IOS Press, 2017, pp. 45-50.

[148] M. J. Assante, „Confirmation of a Coordinated Attack on the Ukrainian Power Grid," SANS ICS, 9 Januar 2016. [Online]. Available: https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid. [Zugriff am 20 November 2019].

[149] J. Hultquist, „Sandworm Team and the Ukrainian Power Authority Attacks," Fireeye, 8 Januar 2016. [Online]. Available: https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html. [Zugriff am 20 November 2019].

[150] F-Secure, BlackEnergy & Quedagh, F-Secure, 2014.

[151] A. Meyers, „CrowdStrike's January Adversary of the Month: VOODOO BEAR," CrowdStrike, 29 Januar 2018. [Online]. Available: https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-january-voodoo-bear/. [Zugriff am 20 November 2019].

[152] F. Herbert, Dune, Vereinigte Staaten: Chilton Books, 1965.

[153] Check Point, „Ukraine Power Outage Demonstrates Infrastructure Vulnerability," Check Point, 18 Januar 2016. [Online]. Available: https://blog.checkpoint.com/2016/01/18/ukraine-power-outage-demonstrates-infrastructure-vulnerability/. [Zugriff am 20 November 2019].

[154] R. Khan, P. Maynard, K. McLaughlin, D. M. Laverty und S. Sezer, „Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid.," in *Proceedings of the 4th International Symposium for ICS \& SCADA Cyber Security Research 2016*, BCS Learning & Development Ltd., 2016, pp. 1-11.

[155] MITRE Corporation, „Sandworm Team," MITRE Corporation, 22 Mai 2018. [Online]. Available: https://attack.mitre.org/groups/G0034/. [Zugriff am 20 November 2019].

[156] P. Polityuk, „Ukraine sees Russian hand in cyber attacks on power grid," Reuters, 12 Februar 2016. [Online]. Available: https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E. [Zugriff am 20 November 2019].

[157] J. Pagliery, „Scary questions in Ukraine energy grid hack," Cable News Network, 18 Januar 2016. [Online]. Available: https://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/. [Zugriff am 20 November 2019].

[158] D. E. Whitehead, K. Owens, D. Gammel und J. Smith, „Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, IEEE, 2017, pp. 1-8.

[159] K. Wilhoit, „KillDisk and BlackEnergy are Not just Energy Sectory Threats," Trend Micro, 11 Februar 2017. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/?_ga=2.8198962.1830474495.1574329078-892811763.1574329078. [Zugriff am 21 November 2019].

[160] US Department of Homeland Security CISA Cyber + Infrastructure, „Cyber-Attack Against Ukrainian Critical Infrastructure (Update A)," US Department of Homeland Security CISA Cyber + Infrastructure, 7 März 2016. [Online]. Available: https://www.eenews.net/assets/2016/07/19/document_ew_02.pdf. [Zugriff am 22 Novmeber 2019].

[161] K. Zetter, „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, 3 März 2016. [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. [Zugriff am 25 November 2019].

[162] V. Kremez, „APT Malware Analysis: BlackEnergy/Додаток1 Excel VBA Dropper," Kremez, Vitali, 18 Januar 2016. [Online]. Available: http://vkremez.weebly.com/cyber-security/apt-malware-analysis-blackenergy1-excel-vba-dropper. [Zugriff am 25 November 2019].

[163] Electricity Information Sharing and Analysis Center; SysAdmin Audit Network Security, Analysis of the Cyber Attack on the Ukrainian Power Grid, Washington: Electricity Information Sharing and Analysis Center, 2016.

[164] Fireeye, „Cyber Attacks on the ukrainian Grid: What you should know," 2016. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf. [Zugriff am 25 November 2019].

[165] B. Urmersbach, „Ukraine: Gesamtbevölkerung von 2008 bis 2018," Statista, 9 August 2019. [Online]. Available: https://de.statista.com/statistik/daten/studie/232387/umfrage/gesamtbevoelkerung-in-der-ukraine/. [Zugriff am 26 November 2019].

[166] E. D. Borghard und J. Schneider, „Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal.," The Washington Post, 9 Mai 2019. [Online]. Available: https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/. [Zugriff am 10 Dezember 2019].

[167] Encyclopaedia Britannica Inc, „Hamas palestinian nationalist movement," Encyclopaedia Britannic Inc, 17 Januar 2019. [Online]. Available: https://www.britannica.com/topic/Hamas. [Zugriff am 2019 Dezember 2019].

[168] S. Cropsey, „Hamas Cyber Attack and Israel's Armed Response," RealClearDefense.com, 9 Mai 2019. [Online]. Available: https://www.realcleardefense.com/articles/2019/05/09/israel_response_to_hamas_cyber_attack_prompts_armed_response_114410.html. [Zugriff am 10 Dezember 2019].

[169] Israel Defense Forces, „HamasCyberHQ.exe removed," Twitter, 5 Mai 2019. [Online]. Available: https://twitter.com/IDF/status/1125066395010699264. [Zugriff am 10 Dezember 2019].

[170] Israel Defense Forces, „Operational Update," Twitter, 5 Mai 2019. [Online]. Available: https://twitter.com/IDF/status/1125114073987846149. [Zugriff am 10 Dezember 2019].

[171] OASIS Open, „Introduction to STIX," OASIS Open, 2017-2018. [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro. [Zugriff am 20 Februar 2020].

[172] S. Papageorgiou, „Stix-2.0-Editor,“ 20 Dezember 2018. [Online]. Available: https://github.com/SakisPap/Stix-2.0-Editor. [Zugriff am 20 Februar 2020].

[173] OASIS Open, „STIX Visualizer,“ OASIS Open, [Online]. Available: https://oasis-open.github.io/cti-stix-visualization/. [Zugriff am 20 Februar 2020].

[174] B. Schneier, „Schneier on Security,“ Bruce Schneier, 23 Februar 2016. [Online]. Available: https://www.schneier.com/blog/archives/2016/02/practical_tempe.html. [Zugriff am 7 August 2019].

Anhang A

Beispielimplementierung des cyber-terroristischen Angriffs auf Estland (2007) in STIX 2.0:


```
{
    "type": "bundle",
    "id": "bundle--e6ffde04-70e3-4066-8341-d110365cdff8",
    "spec_version": "2.0",
    "objects": [
        {
            "type": "attack-pattern",
            "id": "attack-pattern--a0c03541-7e2d-4584-80f6-68d28c66756d",
            "created": "2020-02-20T13:59:42.843Z",
            "modified": "2020-02-20T13:59:42.843Z",
            "name": "Denial of Service",
            "description": "Hauptäschlich wurden estnische Services mit Denial
of Service Angriffen lahmgelegt."
        },
        {
            "type": "campaign",
            "id": "campaign--72e42b9b-7a28-466a-b8ae-1e96dc486fef",
            "created": "2020-02-20T14:04:39.196Z",
            "modified": "2020-02-20T14:04:39.196Z",
            "name": "Angriffe auf Estland nach Versetzen des Bronzesoldaten",
            "description": "Einige estnische Internetservices von
verschiedensten Zielen wurden im Jahr 2007 von zahlreichen Anfragen überflutet
und funktionierten nicht mehr.",
            "first_seen": "2007-02-20T00:00:00Z",
            "last_seen": "2007-02-20T00:00:00Z",
            "objective": "Proteste gegen das Versetzen eines Monuments"
        },
        {
            "type": "identity",
            "id": "identity--5763c936-3f11-4e7b-b8d2-0d7c222f089e",
            "created": "2020-02-20T14:08:30.068Z",
            "modified": "2020-02-20T14:08:30.068Z",
            "name": "Regierung Estlands",
            "description": "Zu der Regierung Estlands zählen Premierminister,
Parlament, Polizei, lokale Regierungen und politische Parteien. ",
            "identity_class": "organization",
            "sectors": [
                "government-national",
                "government-regional",
                "government-local",
                "government-public-services"
            ]
        },
        {
            "type": "identity",
            "id": "identity--9af21a8d-5cdd-4616-850d-7747d7c35c1d",
```

```
            "created": "2020-02-20T14:09:01.532Z",
            "modified": "2020-02-20T14:09:01.532Z",
            "name": "Banken",
            "identity_class": "organization",
            "sectors": [
                "financial-services"
            ]
        },
        {
            "type": "identity",
            "id": "identity--891062ac-57aa-4c68-9bab-a07afbddabc8",
            "created": "2020-02-20T14:09:30.685Z",
            "modified": "2020-02-20T14:09:30.685Z",
            "name": "Internet Service Provider",
            "identity_class": "organization",
            "sectors": [
                "telecommunications"
            ]
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--9728005a-b4b1-4f24-8802-98b106b5a0c6",
            "created": "2020-02-20T14:23:37.769Z",
            "modified": "2020-02-20T14:23:37.769Z",
            "name": "Russische Sympathisanten",
            "description": "Alle Angreifer, die von der Kreml Jugend dazu
bewegt werden konnten, Denial of Service Angriffe gegen Estland zu starten.",
            "roles": [
                "agent",
                "independent"
            ],
            "resource_level": "individual",
            "primary_motivation": "revenge",
            "secondary_motivations": [
                "unpredictable"
            ],
            "personal_motivations": [
                "unpredictable"
            ],
            "labels": [
                "terrorist"
            ]
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--8b6d1a67-5fd5-4840-8923-c0e0237db7fb",
            "created": "2020-02-20T14:18:11.751Z",
            "modified": "2020-02-20T14:18:11.751Z",
            "name": "Kreml Jugend Naschi",
            "description": "Die einzige Organisation die sich zum Angriff
bekannt hat und ihn vermutlich koordiniert hat.",
```

```
            "roles": [
                "director"
            ],
            "resource_level": "government",
            "primary_motivation": "revenge",
            "labels": [
                "terrorist",
                "nation-state"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--b89a4b17-e385-4818-b6c9-ce156d8b54a2",
            "created": "2020-02-20T14:30:59.302Z",
            "modified": "2020-02-20T14:30:59.302Z",
            "relationship_type": "uses",
            "source_ref": "threat-actor--9728005a-b4b1-4f24-8802-98b106b5a0c6",
            "target_ref": "attack-pattern--a0c03541-7e2d-4584-80f6-
68d28c66756d"
        },
        {
            "type": "relationship",
            "id": "relationship--b543c048-b8a6-499b-9c34-20b43f8d4c31",
            "created": "2020-02-20T14:31:56.723Z",
            "modified": "2020-02-20T14:31:56.723Z",
            "relationship_type": "targets",
            "source_ref": "attack-pattern--a0c03541-7e2d-4584-80f6-
68d28c66756d",
            "target_ref": "identity--891062ac-57aa-4c68-9bab-a07afbddabc8"
        },
        {
            "type": "relationship",
            "id": "relationship--39354682-6f57-4f0a-9035-001a8e18989a",
            "created": "2020-02-20T14:51:34.001Z",
            "modified": "2020-02-20T14:51:34.001Z",
            "relationship_type": "instigate",
            "source_ref": "threat-actor--8b6d1a67-5fd5-4840-8923-c0e0237db7fb",
            "target_ref": "threat-actor--9728005a-b4b1-4f24-8802-98b106b5a0c6"
        },
        {
            "type": "relationship",
            "id": "relationship--79d83e48-7a69-488e-96fd-a3b73c2a5fd2",
            "created": "2020-02-20T14:31:39.789Z",
            "modified": "2020-02-20T14:31:39.789Z",
            "relationship_type": "targets",
            "source_ref": "attack-pattern--a0c03541-7e2d-4584-80f6-
68d28c66756d",
            "target_ref": "identity--5763c936-3f11-4e7b-b8d2-0d7c222f089e"
        },
        {
            "type": "relationship",
```

```
            "id": "relationship--cd2390f3-c0c1-48af-a2a0-bcc0bb51f4b5",
            "created": "2020-02-20T14:30:35.242Z",
            "modified": "2020-02-20T14:30:35.242Z",
            "relationship_type": "attributed-to",
            "source_ref": "campaign--72e42b9b-7a28-466a-b8ae-1e96dc486fef",
            "target_ref": "threat-actor--8b6d1a67-5fd5-4840-8923-c0e0237db7fb"
        },
        {
            "type": "relationship",
            "id": "relationship--e0ec171f-f117-4312-a1a3-4ee0fec9272d",
            "created": "2020-02-20T14:31:48.729Z",
            "modified": "2020-02-20T14:31:48.729Z",
            "relationship_type": "targets",
            "source_ref": "attack-pattern--a0c03541-7e2d-4584-80f6-
68d28c66756d",
            "target_ref": "identity--9af21a8d-5cdd-4616-850d-7747d7c35c1d"
        },
        {
            "type": "relationship",
            "id": "relationship--2f0bfc39-3818-4623-9eae-bcc64eb83d0b",
            "created": "2020-02-20T14:34:52.027Z",
            "modified": "2020-02-20T14:34:52.027Z",
            "relationship_type": "attributed-to",
            "source_ref": "campaign--72e42b9b-7a28-466a-b8ae-1e96dc486fef",
            "target_ref": "threat-actor--9728005a-b4b1-4f24-8802-98b106b5a0c6"
        }
    ]
}
```


Beispielimplementierung des cyber-terroristischen Angriffs auf die Ukraine (2015) in STIX 2.0:


```
{
    "type": "bundle",
    "id": "bundle--cfb840bc-f92f-4935-8d9f-a062f6d0d911",
    "spec_version": "2.0",
    "objects": [
        {
            "type": "attack-pattern",
            "id": "attack-pattern--0798db74-dbc4-4b51-9a58-3c05f9bef2a0",
            "created": "2020-02-20T15:36:23.876Z",
            "modified": "2020-02-20T15:36:23.876Z",
            "name": "Phishing",
            "description": "Mithilfe einer Phishing Mail gelang es den
Angreifern die Malware BlackEnergy auf den Systemen der Stromversorger zu
installieren."
        },
        {
            "type": "campaign",
            "id": "campaign--3d3fe9bb-502b-4612-a00c-2386f0a96fcc",
            "created": "2020-02-20T15:41:05.973Z",
            "modified": "2020-02-20T15:41:05.973Z",
```

```
            "name": "Angriffe auf ukrainische Stromversorger",
            "description": "Im Jahr 2014 wurden drei ukrainische Stromversorger
von Cyber-Terroristen angegriffen, welche die Stromversorgung von etwa 225 000
Personen in der Ukraine strten."
        },
        {
            "type": "identity",
            "id": "identity--63deb233-698e-4756-8f66-4a8845512cb2",
            "created": "2020-02-20T15:42:39.469Z",
            "modified": "2020-02-20T15:42:39.469Z",
            "name": "Ukrainische Stromversorger",
            "description": "Die betroffenen Stromversorger waren
Prykarpattiaoblenergo, Chernivtsioblenergo, Kyivoblenergo",
            "identity_class": "organization",
            "sectors": [
                "energy"
            ]
        },
        {
            "type": "indicator",
            "id": "indicator--357e4f05-ed11-4f5b-8e74-46b71184ee87",
            "created": "2020-02-20T15:55:52.976Z",
            "modified": "2020-02-20T15:55:52.976Z",
            "name": "Referenzen zum Roman Dune in der Malware",
            "description": "Die Malware der Angreifer entählt Referenzen zum
Roman Dune. Entsprechende Begriffe können aus dem Roman entnommen werden und
durch den Platzhalter Dune aus dem Pattern erstetzt werden.",
            "pattern": "[file:contains_refs[*].name = 'Dune']",
            "valid_from": "2020-02-20T07:42:50Z",
            "labels": [
                "attribution"
            ]
        },
        {
            "type": "malware",
            "id": "malware--315a85af-8173-42a4-89aa-e6a3a39c1f78",
            "created": "2020-02-20T15:59:36.397Z",
            "modified": "2020-02-20T15:59:36.397Z",
            "name": "Black Energy",
            "labels": [
                "backdoor",
                "remote-access-trojan"
            ]
        },
        {
            "type": "threat-actor",
            "id": "threat-actor--f36e4ddb-893e-454d-b04e-3d3b2652911b",
            "created": "2020-02-20T16:03:59.073Z",
            "modified": "2020-02-20T16:03:59.073Z",
            "name": "Sandworm Team",
```

```
            "description": "Russische Hackergruppe die bei den
Aufklärungsarbeiten bei den Angriffen auf ukrainische Stromversorger als
wahrscheinlichster Angreifer identifiziert wurde.",
            "aliases": [
                "Quedagh,",
                "Voodoo Bear"
            ],
            "roles": [
                "agent",
                "director",
                "malware-author"
            ],
            "sophistication": "strategic",
            "labels": [
                "terrorist"
            ]
        },
        {
            "type": "tool",
            "id": "tool--363d61de-8168-4ca1-8b83-6d21fccb38db",
            "created": "2020-02-20T16:04:56.993Z",
            "modified": "2020-02-20T16:04:56.993Z",
            "name": "Remote Desktop Protocol",
            "labels": [
                "remote-access"
            ]
        },
        {
            "type": "tool",
            "id": "tool--b3febb55-662e-40e5-9617-1c934d6b287c",
            "created": "2020-02-20T16:06:19.979Z",
            "modified": "2020-02-20T16:06:19.979Z",
            "name": "Secure Shell",
            "labels": [
                "remote-access"
            ]
        },
        {
            "type": "tool",
            "id": "tool--e0170164-7a3c-4768-a61b-f02cac04a055",
            "created": "2020-02-20T16:05:22.010Z",
            "modified": "2020-02-20T16:05:22.010Z",
            "name": "Remote Administrator",
            "labels": [
                "remote-access"
            ]
        },
        {
            "type": "relationship",
            "id": "relationship--9f574861-e555-4e55-a024-9563fe0da2dd",
            "created": "2020-02-20T16:08:43.054Z",
```

```
            "modified": "2020-02-20T16:08:43.054Z",
            "relationship_type": "targets",
            "source_ref": "tool--e0170164-7a3c-4768-a61b-f02cac04a055",
            "target_ref": "identity--63deb233-698e-4756-8f66-4a8845512cb2"
        },
        {
            "type": "relationship",
            "id": "relationship--0145c57e-3752-416a-9f34-455e98c6be57",
            "created": "2020-02-20T16:08:38.091Z",
            "modified": "2020-02-20T16:08:38.091Z",
            "relationship_type": "targets",
            "source_ref": "tool--b3febb55-662e-40e5-9617-1c934d6b287c",
            "target_ref": "identity--63deb233-698e-4756-8f66-4a8845512cb2"
        },
        {
            "type": "relationship",
            "id": "relationship--b2853be1-2ba8-49d3-b0ae-7d95ce9bbb34",
            "created": "2020-02-20T16:08:31.741Z",
            "modified": "2020-02-20T16:08:31.741Z",
            "relationship_type": "targets",
            "source_ref": "tool--363d61de-8168-4ca1-8b83-6d21fccb38db",
            "target_ref": "identity--63deb233-698e-4756-8f66-4a8845512cb2"
        },
        {
            "type": "relationship",
            "id": "relationship--b69d116e-0339-4c44-8d13-ec11cca333b9",
            "created": "2020-02-20T16:07:50.059Z",
            "modified": "2020-02-20T16:07:50.059Z",
            "relationship_type": "uses",
            "source_ref": "threat-actor--f36e4ddb-893e-454d-b04e-3d3b2652911b",
            "target_ref": "tool--b3febb55-662e-40e5-9617-1c934d6b287c"
        },
        {
            "type": "relationship",
            "id": "relationship--aade0328-83d3-4a33-8bde-d5e548456151",
            "created": "2020-02-20T16:07:03.338Z",
            "modified": "2020-02-20T16:07:03.338Z",
            "relationship_type": "attributed-to",
            "source_ref": "campaign--3d3fe9bb-502b-4612-a00c-2386f0a96fcc",
            "target_ref": "threat-actor--f36e4ddb-893e-454d-b04e-3d3b2652911b"
        },
        {
            "type": "relationship",
            "id": "relationship--c1939d80-4783-42ef-88bf-f49f03842c08",
            "created": "2020-02-20T16:09:01.202Z",
            "modified": "2020-02-20T16:09:01.202Z",
            "relationship_type": "indicates",
            "source_ref": "indicator--357e4f05-ed11-4f5b-8e74-46b71184ee87",
            "target_ref": "threat-actor--f36e4ddb-893e-454d-b04e-3d3b2652911b"
        },
        {
```

```
            "type": "relationship",
            "id": "relationship--9ed23e7d-a9e4-4cb4-9457-048fde29f9fc",
            "created": "2020-02-20T16:07:58.506Z",
            "modified": "2020-02-20T16:07:58.506Z",
            "relationship_type": "uses",
            "source_ref": "threat-actor--f36e4ddb-893e-454d-b04e-3d3b2652911b",
            "target_ref": "tool--e0170164-7a3c-4768-a61b-f02cac04a055"
        },
        {
            "type": "relationship",
            "id": "relationship--a0f7687e-886e-43f1-a5e3-b0da6598ed6c",
            "created": "2020-02-20T16:21:29.336Z",
            "modified": "2020-02-20T16:21:29.336Z",
            "relationship_type": "Contains",
            "source_ref": "malware--315a85af-8173-42a4-89aa-e6a3a39c1f78",
            "target_ref": "indicator--357e4f05-ed11-4f5b-8e74-46b71184ee87"
        },
        {
            "type": "relationship",
            "id": "relationship--fb063d06-7b61-42cb-8d29-50cc86619a98",
            "created": "2020-02-20T16:07:22.670Z",
            "modified": "2020-02-20T16:07:22.670Z",
            "relationship_type": "uses",
            "source_ref": "threat-actor--f36e4ddb-893e-454d-b04e-3d3b2652911b",
            "target_ref": "attack-pattern--0798db74-dbc4-4b51-9a58-
3c05f9bef2a0"
        },
        {
            "type": "relationship",
            "id": "relationship--566595e6-dce8-495f-88ad-28fa375fea8a",
            "created": "2020-02-20T16:07:41.594Z",
            "modified": "2020-02-20T16:07:41.594Z",
            "relationship_type": "uses",
            "source_ref": "threat-actor--f36e4ddb-893e-454d-b04e-3d3b2652911b",
            "target_ref": "tool--363d61de-8168-4ca1-8b83-6d21fccb38db"
        },
        {
            "type": "relationship",
            "id": "relationship--e9b50a8c-81c8-4b91-b12a-b9e709e28053",
            "created": "2020-02-20T16:11:07.130Z",
            "modified": "2020-02-20T16:11:07.130Z",
            "relationship_type": "targets",
            "source_ref": "attack-pattern--0798db74-dbc4-4b51-9a58-
3c05f9bef2a0",
            "target_ref": "identity--63deb233-698e-4756-8f66-4a8845512cb2"
        },
        {
            "type": "relationship",
            "id": "relationship--cf9d9471-2d38-4d7a-a74c-6c4a30240536",
            "created": "2020-02-20T16:23:35.281Z",
            "modified": "2020-02-20T16:23:35.281Z",
```

```
            "relationship_type": "targets",
            "source_ref": "malware--315a85af-8173-42a4-89aa-e6a3a39c1f78",
            "target_ref": "identity--63deb233-698e-4756-8f66-4a8845512cb2"
        }
    ]
}
```