Oktober 2018 · Dr. Sven Herpig und Julia Schuetze,
Mitarbeit Jonathan Jones

Der Schutz von Wahlen in vernetzten Gesellschaften

Wie sich die Sicherheit daten-intensiver Wahlen erhöhen lässt

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Geheimdienste und politische Gruppen haben schon immer versucht, Einfluss auf Wahlen und Wahlkämpfe zu nehmen, um Regierungen zu destabilisieren oder einzelne politische Kandidaten zu stärken. Mit der Digitalisierung sind neue Angriffsmöglichkeiten entstanden. Ein zentrales Sicherheitsrisiko stellen die während einer Wahl verwendeten, immer größeren Datenmengen und sensiblen Informationen dar: Die interne Kommunikation von Wahlkampfzentralen politischer Parteien, Daten über das Verhalten von Wähler:innengruppen in sozialen Netzwerken oder öffentliche Informationsangebote für Wähler:innen können gestohlen, geleaked, manipuliert oder blockiert werden. Angreifer nutzen die Schwachstellen datenintensiver Wahlen immer häufiger aus, wie Zwischenfälle während der US-Präsidentschaftswahl 2016, der Wahl des französischen Präsidenten 2017 oder den Parlamentswahlen in den Niederlanden zeigen.

Es ist davon auszugehen, dass sich digitale Angriffe auf Wahlen in den nächsten Jahren weiter fortsetzen und technisch versierter werden. Regierungen sind bisher kaum auf die neue Gefährdungslage vorbereitet. Zwar werden einzelne Maßnahmen ergriffen, um etwa staatliche IT-Systeme zu schützen, die unmittelbar für die Durchführung eines Wahlgangs benötigt werden. Allerdings reicht die Erhöhung technischer Sicherheitsstandards allein nicht aus, um datenintensive Wahlen besser zu schützen. Benötigt werden Strategien, wie der Staat die Sicherheit der gesamten Wahl und der darin erfassten Daten erhöhen kann – sei es bei Parteien, politische Gruppen, Medienhäusern, relevanten Unternehmen und den im Netz stattfindenden politischen Debatten.

Politische Entscheidungsträger:innen, die solche Strategien entwickeln, sollten sich in einem ersten Schritt einen umfassenden Überblick über die sicherheitspolitischen Herausforderungen datenintensiver Wahlen verschaffen. Dafür ist es zunächst wichtig, die unterschiedlichen Motive hinter den Angriffen zu verstehen. Cyber-Angriffe können im schwerwiegendsten Fall das Ziel haben, das Ergebnis einer Wahl zu beeinflussen, in dem etwa die Stimmauszählung manipuliert wird, um eine einzelne Partei oder ein:e Kandidat:in zu stärken oder zu schwächen. Andere Angriffe können darauf abzielen, dass Vertrauen in eine Wahl zu untergraben, sodass Bürger:innen die Legitimität eines Wahlergebnisses anzweifeln und so politische Spannungen entstehen oder verstärkt werden – ein Effekt der unter anderem erreicht wird, wenn Teile der Wahl durch Angriffe gestört und wiederholt werden müssen. Wiederum andere Operationen können versuchen, Politi-

ker:innen oder politische Gruppen in der Gesellschaft öffentlich zu diskreditieren, eine amtierende Regierung einzuschüchtern oder das internationale Ansehen eines Staates zu beschädigen.

Genauso unterschiedlich wie die Ziele sind die Taktiken und Vorgehensweisen, mit denen Angriffe auf Wahlen stattfinden. Bei sogenannten *Denial-Attacken* wird der Zugang zu Daten blockiert, um etwa den Informationsfluss zwischen Wähler:innen und Kandidat:innen zu stören. Ein Beispiel hierfür ist ein Angriff, der 2017 während den niederländischen Parlamentswahlen eine öffentlich finanzierte Website lahmlegte, die viele Wähler:innen nutzten, um sich über die angetretenen Kandidat:innen zu informieren. Bei sogenannten *Manipulations-Angriffen* dringen Angreifer in IT-Systeme ein, um Daten auf Wahlcomputern oder Wähler:innenverzeichnisse zu ändern. Ein solcher Fall ereignete sich 2014 während der Wahl in der Ukraine. Bei *Ausspähungs-Operationen* setzen sich Angreifer in den Netzwerken ihrer Ziele fest, um die Kommunikation innerhalb einer Organisation zu überwachen oder über Hintertüren sensible Daten zu stehlen. Weitere Taktiken sind das *Veröffentlichen* oder *"Leaking"* schädlicher Informationen, *Erpressung* mithilfe erbeuteter Daten oder *Überzeugungs-Kampagnen*.

Datenbestände, die für Angreifer und damit für die Sicherheit von Wahlen von Bedeutung sind, werden nicht zentral gesammelt, sondern umfassen verschiedene Formen von Daten, die verstreut bei Unternehmen, Behörden, Forschungseinrichtungen oder auch auf Privatcomputern verfügbar sind. *Öffentlich zugänglich Wahldaten* sind frei abrufbar und umfassen je nach Staat beispielsweise Adressen von Wahlbüros, Ergebnisse repräsentativer Umfragen oder Abstimmungsergebnisse. Entscheidend bei dieser Form von Daten ist es, dass der öffentliche Zugang zu diesen Daten während einer Wahl nicht gestört werden darf und dass Informationen nicht manipuliert wurden. Neben öffentlichen Wahl-Daten sind auch *Personenbezogene Daten* sicherheitsrelevant. Behörden sammeln große Mengen persönlicher Daten, mit denen sich Wähler:innen identifizieren und ansprechen lassen. In mehreren lateinamerikanischen Staaten wurde Daten dieses Typs bereits entwendet. Dabei handelte es sich um Datenbanken mit Email-Adressen, die dann im Wahlkampf für Desinformationskampagnen missbraucht wurden. Andere Daten-Formen, die für Angriffe auf Wahlen genutzt werden, umfassen von *Behörden ausgestellte Daten, vertrauliche Kommunikation, Sicherheitsdaten* und *Selbstangaben*.

Angreifer finden stets Wege zur Umgehung der von den Dateninhaber:innen gewählten Sicherheitsmaßnahmen. Deren Strategie geht überdies auch dann auf und kann einer Wahl nachhaltig Schaden zufügen, wenn die Ope-

ration nicht erfolgreich ist: Die Kompromittierung von Vertraulichkeit ist unumkehrbar. Für Strategien zum Schutz von Wahlen sind daher neben der Erhöhung technischer Sicherheitsstandards genauso solche Maßnahmen entscheidend, die den Schaden erfolgreicher Angriffe verringern und die Widerstandsfähigkeit der Demokratie insgesamt verbessern. Hierzu zählt beispielsweise Programme für das Sicherheitstraining von Schlüsselakteuren im Wahlprozess, Kommunikationsstrategien für den Umgang mit Zwischenfällen, internationale Zusammenarbeit zwischen Regierungen und Wahl-Behörden oder die Durchführung von Informationskampagnen in der Bevölkerung. Insgesamt sollte dem Schutz von Wahlen innen- wie außenpolitisch mehr Aufmerksamkeit geschenkt werden und als Frage der nationalen Sicherheit behandelt werden.

Danksagung

Diese Analyse wurde von den Mitglieder:innen des Transatlantic Cyber Forum im Rahmen einer Online Zusammenarbeit und gemeinsamer Workshops in Washington D.C. und Berlin unterstützt. Die vertretenen Meinungen und Positionen sind allein die der Autoren und geben nicht notwendigerweise die Meinung der Arbeitsgruppe oder der jeweiligen Arbeitgeber wider. Besonderer Dank gilt:

1. Emefa Addo Agawu, New America
2. Geysha Gonzalez, Eurasia Center, Atlantic Council
3. Stefan Heumann, Stiftung Neue Verantwortung e.V.
4. Joseph Lorenzo Hall, Center for Democracy & Technology
5. James Lewis, Center for Strategic and International Studies, Washington
6. Marco Macori, Institute for Security and Safety (ISS) Hochschule Brandenburg
7. Nemanja Malisevic, Microsoft
8. Tim Maurer, Carnegie Endowment for International Peace
9. Igor Mikolic-Torreira, RAND Corporation
10. Thomas Reinhold, Institute for Peace Research and Security Policy Hamburg/ cyberpeace.org
11. Laura Rosenberger, Alliance for Securing Democracy, The German Marshall Fund of the United States
12. Bruce Schneier, Harvard Kennedy School
13. Isabel Skierka, Digital Society Institute at ESMT Berlin

Inhalt

Einführung

Disclaimer: Es handelt sich bei diesem Papier um eine Übersetzung aus dem englischen Original . Aufgrund der Komplexität des Sachverhalts kann es vereinzelt zu Unstimmigkeiten der beiden Versionen kommen – in diesem Fall gilt das englische Original.

Wahlen sind der Grundpfeiler jeder Demokratie. Die Verwundbarkeit von Wahlen hat angesichts der umfassenden Digitalisierung von Wahlen und der Wahlinfrastruktur im vergangenen Jahrzehnt enorm zugenommen. Die Gewährleistung freier und fairer Wahlen und damit der Schutz vor der Einflussnahme Dritter, ist unverzichtbar für jede Demokratie. Die vorliegenden Analyse bezieht sich auf Einflussnahme, die durch Hacking versucht wird, und zwar unabhängig davon, ob die Aktivitäten von inländischen oder ausländischen Angreifer:innen ausgehen. Andere Studien haben stärker die Desinformation als Mittel der Einflussnahme ins Zentrum gerückt. Im vorliegenden Papier konzentrieren wir uns auf Motive, Methoden von Cyber-Angriffen und die Angriffsflächen, die moderne Wahlen bieten. Der Schutz von Wahlen bedeutet wesentlich mehr als die informationstechnische Sicherheit von Wahlmaschinen. Das vorliegende Papier vertritt im Kern die These, dass es sich um den Schutz von Daten handelt, die für verschiedene Aktivitäten bei der gesamten Wahl von der Vorbereitung über den Wahlkampf bis zur Stimmabgabe genutzt werden. All diese Daten können potenziell ausgenutzt und missbraucht werden. Deswegen gehört zum Schutz von Wahlen die Sicherheit von Daten, aber auch die Konzeption von schadensbegrenzenden Maßnahmen für den Fall, dass getroffene Sicherheitsmaßnahmen versagen. Daher müssen Demokratien nicht nur die informationstechnische Sicherheit verbessern. Sie müssen auch die Resilienz der Gesellschaft gegen Wahlbeeinflussung stärken. Die Art des Problems macht die Beteiligung unterschiedlicher Akteure:innen an der Lösung erforderlich: nur ein gesamtgesellschaftlicher Ansatz kann zum Ziel führen.

In der modernen repräsentativen Demokratie agieren Politiker:innen und politische Parteien als Vertreter:innen von Bürger:innen. Ihre Legitimation in dieser Rolle als Vertreter:innen erhalten sie durch regelmäßige, freie und faire Wahlen[1]. Wahlen sind daher einer der Grundpfeiler der Demokratie und der Schutz der Wahlen ist für jeden demokratischen Staat notwendig. Zur Wahl in einer demokratischen Gesellschaft gehört dabei mehr als nur die

1 United Nations, Resolution 52/129 Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization sowie Inter-Parliamentary Council, Declaration on Criteria for Free and Fair Elections

Stimmabgabe. Zu freien und fairen Wahlen gehört, dass die Aktivitäten der Kandidaten:innen und ihrer Parteien, ihr gesamter Wahlkampf bis zum Tag der Wahl, sowie die Publikation der Ergebnisse nach der Wahl von tatsächlicher Einflussnahme ebenso frei sind wie vom Anschein einer Beeinflussung von außen. Gerade weil Wahlen einen Grundbaustein der Demokratie bilden, gilt jede Behinderung des individuellen Wahlrechts und jede Manipulation der Wahl als ernste Bedrohung für die Souveränität eines Staates. Das hat in der Vergangenheit allerdings Regierungen nicht davon abgehalten, sich in fremde Wahlen einzumischen[2]. Zur Abschreckung und um sich als Staat vor solchen Übergriffen, wenn sie vorkommen, schützen zu können, wurde die Unverletzlichkeit von Wahlen bereits früh durch nationales und internationales Recht etabliert[3].

Die aktuelle Debatte über den Schutz der Unverletzlichkeit von Wahlen ist daher alles andere als neu. Neu ist allerdings die Bedrohung aus dem Cyber-Raum: vom Ausmaß der möglichen Machprojektion aus der Ferne, bis hin zur schnelleren und effektiveren Verbreitung von Wahl-relevanten Informationen sowie neuartige Mittel der Täuschung von Wähler:innen und Politik. Politische Parteien, der Wahlkampf und die Stimmenzählung werden zunehmend digitalisiert und daher abhängig von Daten. Big Data-Algorithmen kommen zum Einsatz, um Wählerverzeichnisse durchzukämmen und zielgenaue Wahlwerbung über Soziale Medien zu verbreiten. Die Registrierung von Wähler:innen kann online erfolgen ebenso wie, je nach Land, am Ende die Stimmabgabe selbst. Der Wahlprozess ist mit neuer Technologie durchsetzt. Daten getriebene Verfahren sorgen für mehr Effizienz und einen leichteren Zugang zur Wahl. Die fortschreitende Digitalisierung von Wahlen macht den demokratischen Prozess allerdings auch angreifbarer und führt zu immer neuen Schwachstellen für die Einflussnahme auf Wahlen durch Cyber-Angriffe.

Die Angreifer:innen bedienen sich dabei der besonderen Charakteristiken des Cyber-Raums, der ihnen ein hohes Maß an Anonymität und Flexibilität für ihre Kampagnen erlaubt. Wie wichtig es ist, diese Bedrohungen zu adressieren, zeigen Prognosen über die fortlaufende Verfeinerung und Anpassung

2 Scott Shane, Russia Isn't the Only One Meddling in Elections. We Do It, Too

3 "Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State" – United Nations, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (Declaration on Friendly Relations) und Jacqueline Van De Velde, The Law of Cyber Interference in Elections

von Angriffstechniken und Methoden[4]. Wenn außerdem Cyber-Angriffe zur Beeinflussung von Wahlen greifbare Erfolge bringen, könnte die Auswirkung sein, dass sich mehr und mehr Staaten und nicht-staatliche Akteure:innen, die notwendigen Kenntnisse und Werkzeuge für solche Kampagnen beschaffen. Die Floskel, dass generell Cyber-Angriffe der Cyber-Abwehr immer einen Schritt voraus sind, trifft auf Wahlverfahren in besonderem Maß zu. Dafür gibt es mehrere Gründe. Erstens, auch fehlgeschlagene Versuche, oder die Behauptung von Wahlmanipulation durch Cyber-Angriffe, einmal öffentlich geworden, kann genügen um die Legitimität der Wahl ins Wanken zu bringen. Entscheidend ist, dass die Wahl als angreifbar wahrgenommen wird. Diejenigen, die für den Schutz der Wahl zu sorgen haben, sind, setzt das zusätzlich unter Druck. Ein weiterer Nachteil ist, dass die Maßnahmen zur Abwehr größtenteils noch nicht zur Verfügung stehen beziehungsweise zu wenig erforscht sind.

Regierungen und zentrale Akteure bei Wahlen weltweit bleiben schlecht vorbereitet gegen Wahlbeeinflussung durch Cyber-Angriffe[5]. Die Investitionen in den Schutz von Wahlen gegen Cyber-Angriffe war hier in der Vergangenheit unzureichend[6]. Der erfolgreiche Angriff auf das Democratic National Committee (DNC), der Cyber-Angriff und die Verbreitung der Emails von John Podesta, dem Vorsitzenden von Hillary Clintons Kampagne im Präsidentschaftswahlkampf 2016[7], und die darauf aufbauende Desinformationskampagne[8] müssen als Alarmsignal und Aufforderung verstanden werden, strategischer über das Problem nachzudenken. Einige Initiativen tun dies schon[9]. Die Mehrheit konzentriert sich dabei auf den Kampf gegen Desinformation, die Verbesserungen der IT-Sicherheit im Wahlkampf, die Regulierung von Wahlwerbung oder die Erhöhung der IT-Sicherheit der für die Wahlen verwendeten Systeme. Alle genannten Ansätze sind unverzichtbar für den Schutz von Wahlen. Die vorliegende Studie schaut sich das Problem in seiner

4 U.S. Director of National Intelligence report Assessing Russian Activities and Intentions in Recent US Elections

5 Jacqueline Van De Velde, The Law of Cyber Interference in Elections

6 Im extrem hart geführten Wahlkampf um die US-Präsidentschaft 2016 wurde lediglich ein verschwindend geringer Anteil der 2,1 Milliarden Wahlkampfspenden dafür verwendet, die von beiden Lagern verwendeten IT-Systeme abzusichern, siehe – Center for Responsive Politics, 2016 Presidential Race campaign funding by candidate und Center for Responsive Politics, Expenditures Breakdown for the Clinton campaign

7 Sven Herpig, Cyber Operations: Defending Political IT-Infrastructures

8 U.S. Department of Justice, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System

9 Belfer Center for Science and International Affairs, Harvard Kennedy School Defending Digital Democracy Releases New Playbooks for States to Counter Election Cyberattacks and Information Operations

Gesamtheit von einer anderen Perspektive an. Es wird konkret analysiert wie gehackte Daten eine Wahl beeinflussen können. Dafür wurden Daten, die bei einer Wahl relevant sind, in verschiedene Kategorien aufgeteilt. Die Analyse stellt dann die Sicherheit der relevanten Daten in den Mittelpunkt, um die mit Cyber-Angriffen auf diese Daten verbundenen Gefahren für die nationale Sicherheit darzustellen. Daraus werden Empfehlungen für die Verbesserung der nationalen Sicherheit und für die Widerstandsfähigkeit (Resilienz) der Gesellschaft gegen solche Angriffe abgeleitet. Die gesellschaftliche Resilienz gehört neben der technischen Sicherheit zum Kanon der Empfehlungen der Studie, weil man davon ausgehen muss, dass ein:eine planvoll vorgehender Angreifer:in früher oder später in den Besitz Wahl-relevanter Daten kommt und diese ausnutzen kann. Aus diesem Grund dürfen sich die Empfehlungen nicht nur auf IT-Sicherheit beschränken, sondern müssen zwingend unter anderem auch Vorschläge für eine Kommunikationsstrategie enthalten[10]. Regierungen müssen auf den Ernstfall vorbereitet und in der Lage sein, die Legitimität der Wahl jederzeit zu garantieren und entsprechend zu kommunizieren.

Im ersten Abschnitt der Studie werden Gefahrenszenarios dargestellt. Darin werden Intentionen für Angriffe auf die Wahl aus In- und Ausland dargestellt. Im nächsten Schritt werden die Angriffstaktiken, die in früheren Wahlen und politischen Prozessen angewendet wurden, aufgezeigt, auch unter dem Gesichtspunkt, wie sie die Informationssicherheit von Wahlen unterminieren. Dabei wird unterschieden zwischen direkten Auswirkungen, denen nur durch eine Erhöhung der Informationssicherheit begegnet werden kann und indirekten Auswirkungen, die durch eine Verbesserung der Resilienz der Gesellschaft zumindest abgeschwächt werden können. Der anschließende Abschnitt stellt die verschiedenen Kategorien von Daten zusammen, die im Rahmen eines Wahlprozesses insgesamt anfallen, und liefert eine Abschätzung, wie und wo potentielle Angreifer:innen auf die verschiedenen Datentypen zugreifen können: handelt es sich um öffentlich zugängliche Daten (z. Bsp. Webseite mit dem Wahlprogramm einer Partei) oder nicht (z. Bsp. interne Wahlkampfstrategien der Parteien). Aus den Daten, die bei einer Wahl die Angriffsfläche bieten, ergeben sich das Bedrohungsszenario im Einzelnen, sowie die daran ausgerichteten Empfehlungen zu IT-Sicherheit und Resilienz. Die Studie schlägt im Ergebnis Maßnahmen zur Verbesserung von IT-Sicherheit und Resilienz vor. Sie empfiehlt einen gesamtgesellschaftlichen Ansatz, der alle einbezieht: Medien, Zivilgesellschaft, akademische Institutionen, Politik, Verwaltung und Unternehmen.

10 Belfer Center for Science and International Affairs, Harvard Kennedy School Defending Digital Democracy Releases New Playbooks for States to Counter Election Cyberattacks and Information Operations

Strategische Motive

Der erste Schritt zum Schutz von Wahlen im Cyber-Raum besteht darin, die Motive der Angreifer:innen zu verstehen. Auch wenn die verschiedenen Motive (einschließlich der geopolitischen) eng miteinander verwoben und schwer zu differenzieren sind, gehen wir in der vorliegenden Studie von fünf Hauptmotiven aus, warum Angreifer:innen datenintensive Wahlen angreifen: Manipulation des Wahlergebnisses, Diskreditierung politischer Akteure, Einschüchterung von Regierungen und Untergraben der internationalen Glaubwürdigkeit. Der vorliegende Abschnitt wirft einen Blick auf die geopolitischen Motive für die Beeinflussung von Wahlverfahren mit Hilfe von Hacking-Werkzeugen. Die Liste der Möglichkeiten legt nahe, dass ein:e Angreifer:in den Vorteil hat, dass bereits der gescheiterte Versuch beispielsweise einer Manipulation des Wahlergebnisses, wenn er öffentlich wird, ausreicht, um das Vertrauen der Öffentlichkeit in den demokratischen Prozess zu erschüttern.

Manipulation des Wahlergebnisses

Die Manipulation des Wahlergebnisses ist die wirkungsmächtigste Art, eine Wahl zu beeinflussen. Diese Art der Manipulation zielt auf die Beeinflussung des Prozesses der Stimmabgabe durch die Bürger:innen ab, nachdem er:sie sich entschieden hat, wen er:sie wählt. Erreicht werden kann dies sowohl durch die Veränderung der Auszählungsergebnisse (auf lokaler, bundesstaatlicher oder nationaler Ebene) oder durch die Veränderung der Wählerverzeichnisse oder der sogenannten E-Poll-Books, so dass ein Teil der eigentlich stimmberechtigten Wähler:innen ihre Stimme nicht mehr für eine bestimmte Partei oder einen:eine bestimmten:bestimmte Kandidaten:Kandidatin abgeben können. Zwei entgegengesetzte Varianten sind denkbar: entweder wird versucht einem:einer bestimmten:bestimmte Politiker:in oder einer bestimmten Partei zum Sieg zu verhelfen oder, wenn es mehr als zwei Wahlmöglichkeiten gibt, wird darauf gesetzt, dass eine bestimmte Partei oder ein:e bestimmter:bestimmte Politiker:in die Wahl verliert. Ein:e Angreifer:in würde dazu ein System attackieren, in dem die entsprechenden Daten gespeichert sind, und die Abstimmergebnisse oder die Daten über die Wähler:innen in den Wählerverzeichnissen ändern, etwa Adresse oder Parteizugehörigkeit. In manchen Ländern führt eine Änderung der Adresse der Wähler:innen dazu, dass sie nicht mehr in ihrem Bezirk abstimmen können oder die Briefwahl unmöglich wird. Wird die gespeicherte Information über die Parteizugehörigkeit verändert, werden Wähler:innen von Parteiwahlen ausgeschlossen, etwa den Vorwahlen im US-Wahlkampf oder von Ur-Ab-

stimmungen über Koalitionen in Deutschland. Angreifer:innen könnten hier zum Beispiel auch IT-Administratoren angreifen/ erpressen, die direkten Zugriff auf die entsprechenden Systeme haben.

Deligitimierung des demokratischen Prozesses

Den demokratischen Prozess seiner Legitimation zu berauben heißt, durch Cyber-Angriffe Zweifel bezüglich des korrekten Funktionierens der Wahl zu säen. Dabei müssen die entsprechenden Angriffe nicht notgedrungen erfolgreich sein. Die Wahrnehmung, dass IT-Systeme und Wahl-Infrastruktur angreifbar oder manipulierbar sind[11], kann dem demokratischen Prozess seine Legitimation (in der Öffentlichkeit) entziehen. Es reicht, dass die Wählerschaft glaubt, dass das Wahlergebnis nicht den „Willen des Volkes“ widerspiegelt. Dieser Effekt kann etwa durch einen Angriff auf Webseiten erzielt werden, die Daten zum Wahlkampf oder zu den antretenden Parteien beinhalten, so dass Wähler:innen auf die entsprechenden Information nicht mehr zugreifen können. Es kann aber auch schlicht die Integrität der entsprechenden Informationen in Zweifel gezogen werden. Ähnliche Angriffe können auf Systeme ausgeführt werden, die Daten zur Authentifizierung von Wähler:innen enthalten, so dass Wähler:innen bei ihrer Stimmabgabe behindert würden. Auch Verzeichnisse über Stimmberechtigte könnten angegriffen oder verändert werden, so dass Wähler:innen daran gehindert werden, ihre Stimme abzugeben[12] oder dies erst nach einer erneuten Verifizierung tun können. Um das Vertrauen in den demokratischen Prozess als solches zu untergraben (anstatt bestimmten Kandidaten:innen oder Parteien zum Sieg zu verhelfen), muss ein Angriff nicht auf einen bestimmten Teil der Wählerschaft ausgerichtet sein (im Vergleich zur vorherigen Motivation). Es reicht, dass der Angriff öffentlich bekannt wird, um die Legitimität des Prozesses zu untergraben. Eine weitere Möglichkeit, das Vertrauen in eine Wahl zu erschüttern, besteht in der öffentlichen Aufdeckung von Schwachstellen bei Wählerverzeichnissen, bei Software zur Stimmauszählung[13] oder bei Wahl-

11 “It has been publicly reported that Russian actors targeted electoral infrastructure in over 20 states prior to the 2016 election. Although there is no evidence indicating that these cyber operations resulted in the disruption of any voting results, the Russian government maintains both the intent and capability to undermine confidence in the integrity of an electoral tally. The need to increase cybersecurity among the nation’s electoral infrastructure, and particularly in voter registration databases and electronic voting machines, has gained heightened salience since the 2016 election”, Suzanne Spaulding, Countering Adversary Threats to Democratic Institutions

12 Nicole Perlroth, Michael Wines and Matthew Rosenberg, Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny

13 Laura Smith-Spark, Hackers warn of flaws in German election software weeks before vote

maschinen. Die Schwachstellen müssen dabei wiederum nicht zwangsläufig ausgenutzt werden. Das Finden und Schließen solcher Schwachstellen ist von größter Bedeutung, eine Veröffentlichung sollte allerdings in einem geordneten Verfahren und gemäß den Maßgaben gut eingespielter Richtlinien zur Bekanntgabe von Schwachstellen – inklusive entsprechender Kommunikationsmaßnahmen – erfolgen.

Alle aufgeführten Arten von Angriffen (s. Annex A) können mit einer gezielten Medien- oder Desinformationskampagne kombiniert werden um dieses Ziel zu erreichen. Zur großen Wirksamkeit trägt nicht nur die Vielzahl an Werkzeugen bei, die dafür zur Verfügung stehen, sondern auch der Umstand, dass einmal verlorenes Vertrauen in den Wahlprozess nur sehr schwer wieder herzustellen ist. Um eine Wahl zu delegitimieren, muss der Angriff nicht erfolgreich sein. Der bloße Anschein, dass der Angriff erfolgreich war oder möglich ist, kann hier genügen um das Ziel zu erreichen[14].

Diskreditierung politischer Akteure

Die Diskreditierung politischer Akteure wie Politiker:innen, Parteien, Interessensgruppen oder der aktuellen Regierung kann ein mächtiges Werkzeug sein, um die öffentliche Meinung zu beeinflussen, und somit ein bestimmtes Wahlergebnis zu forcieren. Die einfachste Möglichkeit ist die Verbreitung von – durch Cyber-Angriffe beschaffte – Informationen oder Dokumenten, die politische Akteur:innen in einem schlechten Licht erscheinen lassen, und die zum Skandal für die entsprechenden Akteur:innen werden können. Auf den ersten Blick mag das sogenannte „Leaken“ von kompromittierenden Dokumenten als schlichte Angriffsvariante erscheinen. Die parallele Verbreitung von Nachrichten mit einem bestimmten Spin und die Ansprache bestimmter, speziell ausgewählter, und potentiell für das Thema empfänglicher Zielgruppen (etwa durch Micro-Targeting) können dafür sorgen, dass auch schon mit wenig Aufwand viel erreicht werden kann. Die Veränderung von Dokumenten und die Mischung von Originaldokumenten mit präparierten Dokumenten kann den Wirkungseffekt eines solchen Angriffs gegebenenfalls noch weiter erhöhen. Außerdem können Webseiten und Konten in Sozialen Medien übernommen werden, um darüber die schädlichen Informationen zu verbreiten. Die Nachteile für das Opfer liegen auf der Hand: Fake News richtig zu stellen

14 Auch wenn es außerhalb des Analyse-Rahmens dieser Arbeit ist, so kann möglicherweise alleine die Behauptung, dass die Wahl-Infrastrukturen erfolgreich gehackt worden sind, zu Gleichen Ergebnissen führen. Hierbei würde es sich dann jedoch ausschließlich um eine Desinformationskampagne ohne Cyber-Angriff handeln.

erfordert Zeit und ist selten so erfolgreich wie deren Verbreitung[15]. Abgesehen von einzelnen Politikern:innern können auch ganze politische Gruppen, etwa die Koalitionäre:Koalitionärinnen einer Regierung, oder das ganze Parteiensystem, das so genannte „Establishment“ diskreditiert werden. Das kann beispielsweise auch dadurch erreicht werden, dass eine gemeinsame politische Idee statt einzelnen Akteuren diskreditiert wird. Die Zugewinne von Parteien der extremen Rechten auf Kosten der etablierten und moderateren Parteien überall in Europa speisen sich unter anderem aus der Diskreditierung der etablierten Politikansätze, unter anderem bei der Bewältigung der Flüchtlingskrise[16]. Angriffe sind nicht nur gegen diese Akteure, sondern auch ihre Unterstützter:innen oder Vertraute denkbar – überall dort wo kompromittierende Informationen vorliegen.

Einschüchterung der Regierung

Cyber-Angriffe auf Wahlen können auch dazu genutzt werden, um die Regierung eines Landes einzuschüchtern. Es kann Ausdruck einer geopolitischen Machtdemonstration sein, und muss nicht zwangsläufig am Wahltag stattfinden, sondern kann während eines Wahlkampfes oder auch während laufender internationaler Verhandlungen erfolgen. Eine solche Machtdemonstration kann verdeckt das Missfallen des:der Angreifers:Angreiferin über die nationale Agenda der betroffenen Regierung zum Ausdruck bringen, oder schlicht die Botschaft senden: „nicht einmal Eure Wahlen sind sicher vor uns“. Die Wahlen in der Ukraine 2014 lieferten ein Beispiel für einen solchen offenen Einschüchterungsversuch mittels eines Cyber-Angriffs. In diesem Fall wurde ein gut koordinierter Angriff von drei verschiedenen Seiten aus gestartet. Zunächst löschten Angreifer vier Tage vor der Präsidentschaftswahl Schlüsselinformationen auf den Rechnern der ukrainischen Wahlkommission[17]. Zwar konnten diese entsprechenden Informationen am folgenden Tag wieder eingespielt werden, doch wenige Minuten vor Bekanntgabe des Wahlergebnisses live im Fernsehen wurde Malware gefunden, deren Ziel die Manipulation des Wahlergebnisses zugunsten des Kandidaten der extremen Rechten war. Der dritte Teil des Angriffs bestand in einer Distributed Denial of Service-Attacke (DDoS) auf das Auszählungssystem, was die Stimmauszählung verzögerte.

15 Soroush Vosoughi Deb Roy and Sinan Aral, The spread of true and false news online
Alexander Sängerlaub, Feuerwehr ohne Wasser?
Alexander Sängerlaub, Miriam Meier and Wolf-Dieter Rühl, Fakten statt Fakes

16 Simon Shuster, European Politics Are Swinging to the Right

17 Mark Clayton, Ukraine election narrowly avoided ‘wanton destruction’ from hackers

Untergraben der Glaubwürdigkeit auf internationale Ebene

Der Verlust an Glaubwürdigkeit in Bezug auf die Abhaltung von Wahlen in einem Land kann zu Problemen bei internationalen Verhandlungen für das betroffene Land führen. Wir heben hier vor, dass zwar empirische Studien fehlen, wenn aber die Integrität der Wahl eines Landes in Zweifel gezogen wird, leidet die Glaubwürdigkeit der gewählten Regierung. Derart geschwächte Regierungen können zur Zielscheibe für nationale und internationale Gegenbewegungen werden. Für den betroffenen Staat können bi- und multilaterale Verhandlungen schwieriger werden, weil die internationalen Partner die Opposition oder den Privatsektor als Gesprächspartner bevorzugen, da sie davon ausgehen, dass die Regierung ihre nationale Agenda nicht umsetzen kann. Im Extremfall kann der Glaubwürdigkeitsverlust sogar zum Ausschluss aus bestimmten internationalen Organisationen führen[18]. Auf internationaler Ebene sind zwei Aspekte bedeutsam und können durch die Beeinflussung einer Wahl von außen erheblich forciert werden. Erstens muss ein Staat in der Lage sein, seinen internationalen Verpflichtungen nachzukommen. Zur Umsetzung dieser Verpflichtungen braucht eine Regierung die Unterstützung im eigenen Land. Diskussionen über Neuwahlen sind dem abträglich. Zweitens müssen andere Regierungen darauf vertrauen können, dass sie durch die Zusammenarbeit nicht riskieren, die eigenen Bevölkerung gegen sich aufzubringen, weil sie mit einer „nicht legitimen“ Regierung verhandeln. Des Weiteren könnte Entwicklungsarbeit des Staates leiden, bei der es um den Aufbau von demokratischen Institutionen geht.

18 European Commission, Conditions of Membership

Angriffstaktiken

In diesem Abschnitt erklären wir verschiedene Taktiken, die bei der Beeinflussung von Wahlen in der Vergangenheit bereits zum Einsatz kamen oder Teil von breit angelegten Kampagnen politischer Einmischung waren. Die Angriffstaktiken werden einzeln oder in Kombination eingesetzt, um die im voran gegangenen Abschnitt dargestellten strategischen Ziele zu erreichen. Das Papier beschränkt sich dabei bewusst auf Angriffe durch Hacking[19], die klassische Angriffsvektoren nutzen[20]. Eine Meinungs- oder Desinformationskampagne wird nur dann einbezogen, wenn sie in Verbindung mit vorausgegangenem Hacking steht. Das ist beispielsweise der Fall, wenn per Micro-Targeting mit gestohlenen Informationen über Wähler:innen gearbeitet wird, oder wenn ein Angriff darin besteht, zuvor durch einen Cyber-Angriff entwendete vertrauliche Informationen zu veröffentlichen. Diese Beschränkung auf Szenarios, die solche Angriffe beinhalten, erlaubt es uns, die CIA Trias[21] zur Grundlage der Analyse zu machen. Die CIA Trias ist ein anerkanntes Konzept der IT-Sicherheitsanalyse und erlaubt eine Bewertung, über die wesentlichen Aspekte der Informationssicherheit, die sogenannten *Schutzziele*. Diese Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit beziehungsweise alle Kombinationen dieser Schutzziele. Wir wenden hier die CIA Prinzipien auf die Sicherheit aller Daten an, die während einer Wahl eine Rolle spielen. Bei der Präsentation der Angriffstaktiken heben wir jeweils hervor, welches Schutzziel Ziel des Angriffs ist.

Man kann bei den Auswirkungen von Cyber-Angriffen auf Wahlen zwischen zwei Kategorien unterscheiden. In die erste Kategorie fallen die unmittelbaren Auswirkungen. Beispiele dafür sind etwa DDoS-Angriffe auf die Webseite eines:einer Kandidaten:Kandidatin, die den Zugriff der Wähler:innen auf diese Seite und die darin über den:die Kandidaten;Kandidatin angebotenen Informationen blockieren. Unmittelbaren Auswirkungen kann mit verbesserten informationstechnischen Absicherungen (etwa Firewalls, Intrusion Detection Software oder Verschlüsselung) begegnet werden.

Die zweite Kategorie von Angriffen richtet keinen unmittelbaren Schaden an, sondern wird erst mittelbar und nachgelagert wirksam. Beispielsweise veröffentlichten Angreifer:innen in der heißen Phase des französischen Prä-

19 Hacking ist hier definiert als “the exploitation of existing vulnerabilities in soft- and hardware and online services to access data in transit and data at rest or manipulate a target’s device (e. g. by switching on sensors or altering existing software)” – Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers

20 Annex A.

21 Chad Perrin, The CIA Triad

sidentschaftswahlkampfes zum Teil offensichtlich manipulierte Informationen, die sie von einem kompromittierten IT-System der Partei des Präsidentschaftskandidaten Emmanuel Macron, En Marche![22] entwendet hatten. Zwar entfaltete der Angriff auf die IT-Systeme keine unmittelbare Wirkung, das „Leaken" der gewonnenen Informationen hatte aber eine nachgelagerte Auswirkung. Eine bessere informationstechnische Absicherung vorab hätte die IT-Systeme der Partei durchaus schützen können. Doch nachdem der Angriff erfolgt war, konnte aus IT-Sicherheitsperspektive nichts mehr gegen die Verbreitung der gestohlenen Informationen getan werden. Der Fall illustriert, warum es für die verteidigende Seite schwierig ist, gute Abwehrstrategien zu entwickeln. Hier werden schadensbegrenzende Maßnahmen werden notwendig, wie beispielsweise strategische Kommunikation. Diese kann dazu beitragen, dass Wahlen Auswirkungen von derartigen Angriffen besser überstehen können. Im Fall des französischen Präsidentschaftswahlkampfes reagierte die Partei durch gezielte strategische Kommunikation auf die mit dem Angriff verbundenen nachgelagerten Auswirkungen. Sie trat den „Leaks" mit einer eigenen Botschaft entgegen, in der sie darauf hinwies, dass die von den Angreifern verwendeten Informationen gefälscht und verändert worden seien.

Verfügbarkeit einschränken

Die Einschränkung der Verfügbarkeit zielt letztlich darauf, Informationen (temporär) unzugänglich zu machen. Webseiten, Soziale Medien, Email-Kontos, Kurznachrichtendienste und IT-Infrastrukturen werden genutzt, um Informationen der Wählerschaft verfügbar zu machen. Ein potentieller:potentielle Angreifer:in kann den Informationsfluss unterbrechen oder einschränken und so den Zugang zu den entsprechenden Informationen durch die Wählerschaft (oder einer Teilgruppe der Wähler:innen) unterbinden. Der Angriff kann sich gegen politische Parteien, Kandidaten:Kandidatinnen oder auch gegen die öffentliche IT-Infrastruktur der Politik allgemein richten, beispielsweise Systeme und Netzwerke, die Informationen für die Wahl bereithalten. Der entsprechende Effekt wurde bewusst oder unbewusst von zwei mutmaßlichen „Hacker-Aktivisten" vor den niederländischen Präsidentschaftswahlen 2017 erzielt. Mit einem DDoS-Angriff blockierten sie den Zugang zu zwei wichtigen, öffentlich finanzierten Webseiten[23]. Die beiden Seiten waren 2012 von fast der Hälfte aller niederländischen Wähler:innen genutzt worden, um sich für einen:eine der Kandidaten:innen zu ent-

22 Andy Greenberg, Hackers hit Macron with huge email leak ahead of French Election

23 Harrison Van Riper, Turk Hack Team and the "Netherlands Operation"

scheiden[24]. Ein aktuelles Beispiel ist auch der Angriff auf Computersysteme in Knox County, Tennessee, wo ein ähnlicher Angriff dazu führte, dass die für den 1. Mai angekündigte Bekanntgabe der Vorwahlergebnisse für lokale Wahlen, darunter für den:die Polizeichef:in und den:die Bürgermeister:in, verzögert wurde[25].

Eine andere Qualität hat eine solche Unterbrechung eines Dienstes, wenn er direkt auf die Funktion der Wahlmaschinen zielt. In einem solchen Fall wird nicht einfach der Zugang zu Informationen für die Bürger:innen eingeschränkt, vielmehr wird die Stimmabgabe behindert. Werden Wahlmaschinen unbrauchbar gemacht, würden Wähler:innen (oder einzelne Wählergruppen) an der Ausübung ihres Wahlrechts behindert. Diese Art des Angriffs kann auf die Integrität der für die Wahlmaschinen notwendigen Daten zielen, auf die Verfügbarkeit der Funktion der Wahlmaschinen, und damit schließlich auf den Prozess der Stimmabgabe. Solche Angriffe haben eine unmittelbare Auswirkung.

Schwächung des Vertrauens

Diese Taktik zielt im Wesentlichen auf die Integrität der für die Wahl notwendigen Daten und die öffentliche Wahrnehmung der Sicherheit der Wahlen ab. Das Vertrauen in das Wahlverfahren zu schwächen kann ein direktes Ziel oder die Folgewirkung eines Cyber-Angriffs sein. Letzteres trifft zu, wenn die Enthüllung eines Angriffs, der ein anderes Ziel hatte Zweifel in der Öffentlichkeit schürt, dass die Integrität der Wahl kompromittiert wurde. In beiden Fällen erzielen die Angreifer:innen durch ihren Angriff eine unmittelbare Auswirkung. Der:die Angreifer:innen können etwa die Verwundbarkeit der Wahlmaschinen demonstrieren[26], auf die Integrität des Wählerverzeichnisses abzielen[27] und die Vertraulichkeit der gespeicherten Daten kompromittieren, oder andere Ziele innerhalb des Wahlsystems finden.

Allein die Vorstellung, dass das Wahlsystem kompromittiert ist, kann das öffentliche Vertrauen erheblich beschädigen. Der Effekt kann verstärkt werden, wenn Akteur:innen (im eigenen Land) einen solchen Angriff für eigene Zwecke ausnutzen wollen. Das von der US-Regierung 2017 veröffentlichte Strategiepapier zur nationalen Sicherheit hebt im Kapitel zum Cyber-Raum

24 Reuters Staff, Dutch voting guide sites offline in apparent cyber attack

25 Travis Dorman, Cyberattack crashes Knox County election website; votes unaffected

26 Adam Lusher, Hackers breached defences of US voting machines in less than 90 minutes

27 James Temperton, The Philippines election hack is ‘freaking huge’

die Bedeutsamkeit dieser Art der Bedrohung besonders hervor[28]. Diese Angriffstaktik eignet sich auch für pure Disruption, zum Beispiel Terrorismus[29], mit der die gesamte Bevölkerung eingeschüchtert werden soll.

Eine schadensmindernde Maßnahme, die hier in Betracht kommt, ist der komplette Verzicht auf elektronische Wahlmaschinen. Deutschland[30], die Niederlande und Norwegen zum Beispiel haben entschieden, keine elektronische Wahlmaschinen einzusetzen, sondern die Stimmen stattdessen manuell auszuzählen[31].

Manipulation

Manipulationen zielen vor allem auf die Integrität von Daten ab. Durch das Ändern von Daten, etwa in den Wählerverzeichnissen, können Angreifer:innen subtil und möglicherweise ohne große Aufmerksamkeit zu erregen, ihre Ziele erreichen. Gerade in Zeiten, in denen Kandidaten:Kandidatinnen im Wahlkampf zunehmend auf die in den Wählerverzeichnissen gespeicherten Daten setzen, um ihre Kampagnen individuell auf Wähler:innen zuzuschneiden[32], sind Datenmanipulationen eine ideale Angriffsstrategie. Diese Art des Angriffs konnte bei den Wahlen in der Ukraine 2014[33] beobachtet werden. Wären die Manipulationen für einige Zeit unbemerkt geblieben, wäre es zunehmend schwierig geworden, die ursprüngliche Form der veränderten Datensätze und Dokumenten wiederherzustellen, obwohl Backups vorhanden waren. Es wäre auf jeden Fall notwendig gewesen, den exakten Zeitpunkt zu wissen, wann die Änderungen vorgenommen wurden.

Die Taktik kann auch vollkommen offen eingesetzt werden, weil sie nicht darauf zielt, die Verfügbarkeit oder Vertraulichkeit von Daten einzuschränken – und sie kann mit einer Persuasions-Kampagne kombiniert werden. Der physikalische Zugriff auf Wahlmaschinen[34] (während des Transports) oder

28 White House, National Security Strategy of the United States of America, December 2017

29 James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War, and other Cyber Threats

30 Bundesverfassungsgericht, Verwendung von Wahlcomputern bei der Bundestagswahl 2005 verfassungswidrig

31 Thomas Nilsen, Norwegian votes to be counted manually in fear of election hacking und Sewell Chan, Fearful of Hacking, Dutch Will Count Ballots by Hand

32 Sasha Issenberg, How Obama's Team Used Big Data to Rally Voters

33 Mark Clayton, Ukraine election narrowly avoided 'wanton destruction' from hackers

34 Lily Hay Newman, To Fix Voting Machines, Hackers Tear Them Apart

der Zugriff auf die eingesetzte Hardware[35] noch während des Herstellungsprozesses sind zwei von mehreren möglichen Methoden, mit denen Wahlmaschinen manipuliert werden können, um später die Stimmverhältnisse zu fälschen oder die Maschinen funktionsunfähig zu machen.

Im Vorfeld der deutschen Wahlen 2017 gelang es Hackern, Schwachstellen in der Software für die Zusammenführung und Übertragung von Auszählungsergebnissen aufzuzeigen[36]. Das Beispiel zeigt, dass es selbst dann Angriffspunkte gibt, wenn eine Wahl auf Papier ausgeführt und manuell ausgezählt wird.

Ein Vertrauensverlust gegenüber der Wahl ist eine mögliche Konsequenz dieser Angriffstaktik. Der Schaden kann unabhängig davon eintreten, ob die Manipulation aufgedeckt und behoben wird.

Ausspähung

Ausspähung richtet sich vor allem gegen die Vertraulichkeit von Daten und etwaige Angriffe versuchen Systeme zu infiltrieren, um später von innen die Entwicklungen zu überwachen und möglicherweise Daten auszuleiten. Ein Nebeneffekt ist die Verletzung der Integrität des Systems, in dem etwa der heimliche Zugriff auf Daten über eine so genannte Backdoor ermöglicht wird. Hierzu gehört auch das Austesten von Sicherheitsmaßnahmen durch die Angreifer:innen. Dieser Angriff kann als Ausgangspunkt für die Angreifer:innen dienen, von dem aus sie weitere Schwachstellen des IT-Zielsystems erkunden und/oder die laufende Kommunikation oder gespeicherte Daten ausspähen können. Ein wichtiges Ziel ist es dabei, den verdeckten Zugang zum System herzustellen, ohne entdeckt zu werden und ihn als Basis für spätere Manipulationen im System auszubauen. Ein weiterer Folgeeffekt dieses Szenario besteht wiederum im Vertrauensverlust für das System, wenn später etwa durch einen Security Audit, offenkundig wird, dass wichtige Teile des IT-Systems oder der Infrastruktur kompromittiert waren. Diese Taktik kam im Präsidentschaftswahlkampf in den USA 2016 zum Einsatz, als Angreifer:innen Wahl relevante Systeme in 21 Bundesstaaten auf Schwachstellen testeten.[37]

35 John Sebes, Elections + National Security = Hardware Threats + Policy Questions

36 46halbe, Software zur Auswertung der Bundestagswahl unsicher und angreifbar

37 Morgan Chalfant, Bipartisan group of lawmakers backs new election security bill

„Leaks“

Das „Leaken“ zielt vor allem auf die Vertraulichkeit von Daten ab. Bei dieser Taktik konzentrieren sich die Angreifer:innen darauf, an kompromittierende Informationen über eine Zielperson zu gelangen und diese dann zu veröffentlichen. Oder sie spielen die erlangten Informationen einer dritten Partei zu, um die Intentionen des:der Angreifer:in zu verschleiern und möglicherweise zugleich die Glaubwürdigkeit des gestohlenen Materials zu erhöhen. Wikileaks bot in der Vergangenheit eine gute Plattform, über die Dokumente veröffentlicht werden konnten, die von kompromittierten Systemen stammten[38]. Auch wenn der beste Ort für die Veröffentlichung der gestohlenen Informationen eine glaubwürdige Plattform ist, funktioniert letzten Endes jede Plattform im Netz, kombiniert mit Emails an Journalisten und einer Verbreitung über Soziale Medien.

Diese Art des Angriffs fand weltweit große Beachtung, als im US Präsidentschaftswahlkampf 2016 zeitlich klug platzierte Veröffentlichungen kompromittierender Informationen die Neutralität der Nominierung des Präsidentschaftsbewerbers durch das Democratic National Committee (DNC) in Zweifel zogen. Die Vorsitzende des DNC trat in der Folge zurück[39]. Dieses Leak in Verbindung mit der Veröffentlichung des Emails von John Podesta trug möglicherweise auch zum knappen Ausgang der Präsidentschaftswahl zu Gunsten des republikanischen Widersachers Donald Trump bei[40]. Der Fall von Emmanuel Macrons „En Marche!“ Partei hat gezeigt, dass gestohlene Daten zusätzlich auch gezielt manipuliert werden können, um größtmöglichen Schaden anzurichten[41]. Macrons Partei war in Bezug auf die notwendige strategische Kommunikation auf einen solchen Fall ganz offenbar vorbereitet[42].

Die eigentlichen Auswirkungen erzielt nicht der Angriff selbst, sondern das Leaken von Informationen, daher handelt es sich hierbei um eine mittelbare Auswirkung. Der Angriff auf den Deutschen Bundestag hat gezeigt, dass ein Angriff nicht zwangsläufig mit einem Leak gestohlener Daten verbunden

38 Joseph Cox, Guccifer 2.0 Claims Responsibility for WikiLeaks DNC Email Dump

39 Edward-Isaac Dovere and Gabriel Debenedetti, Heads roll at the DNC

40 Sven Herpig, Cyber Operations: Defending Political IT-Infrastructures

41 Adam Nossiter, David E. Sanger and Nicole Perlroth, Hackers Came, but the French Were Prepared

42 Andy Greenberg, Hacker Hit Macron with Huge Email Leak Ahead of French Election

sein muss – auch wenn allgemein davon ausgegangen wurde, dass diese während der folgenden Wahlen veröffentlicht werden würden[43].

Persuasion

Bei der Persuasion geht es um die gezielte Überzeugung der Wähler:innen von einer bestimmten politischen Position. Der Unterschied zum Leaking ist, dass die Persuasion auf bestimmte Personen oder Gruppen zugeschnitten ist. Es gibt unterschiedliche Spielarten dieser Taktik. Erstens, können echte Dokumente, die bei einem vorherigen Angriff erbeutet wurden, für breit angelegte Medien- oder Desinformationskampagnen genutzt werden[44]. Das war bei der Veröffentlichung der Emails von John Podesta der Fall[45]. Zudem werden bei der Persuasion auch Methoden des Micro-Targeting eingesetzt, mit denen Falschinformationen unter Zuhilfenahme von zuvor gestohlenen Daten aus den Wählerverzeichnissen gezielt zugeschnitten werden[46]. Schließlich können für die Taktik auch Konten übernommen werden, etwa in Sozialen Medien, wie es dem australischen Verteidigungsminister Pyne 2017 passierte[47].

Die Angriffsmöglichkeiten bei der Persuasion sind breit gefächert, die Auswirkungen beträchtlich und die Methode lässt sich mit vielen anderen Strategien der Wahlbeeinflussung verbinden. Angreifer:innen können an verschiedenen Punkten ansetzen, da die Angriffsfläche sehr groß ist. Aus diesem Grund ist das beste Mittel zur Verteidigung gegen entsprechende Kampagnen eine für diesen Persuasion aufgeklärte, und in dem Sinne resiliente Gesellschaft.

Erpressung

Diese Taktik baut auf die Beschaffung von vertraulichen Informationen auf, um Individuen oder politische Akteure wie Parteien einzuschüchtern. Hack-Mail Angriffe, mit denen sich Angreifer:innen finanziell bereichern wollen, sind außerhalb der Politik bereits hinlänglich bekannt. Man muss aber

43 Sven Herpig, Cyber Operations: Defending Political IT-Infrastructures

44 Desinformationskampagnen werden oft um reale Dokumente und Ereignisse herum gesponnen.

45 Raphael Satter, Inside story: How Russians hacked the Democrats' emails

46 Quelle für die Daten zur politischen Orientierung der einzelnen Bürger:innen kann beispielsweise ein Hersteller von Wahlsystemen sein, wie dies in den USA der Fall war, siehe Matthew Cole, et al, Top Secret NSA Report Details Russian Hacking Efforts days before 2016 Election

47 Fergus Hunter, 'I was hacked!': Christopher Pyne's Twitter account in porn mishap

davon ausgehen, dass sich dieser Modus Operandi künftig mehr und mehr auch für politische Zwecke durchsetzt, besonders angesichts der jüngsten Entwicklungen im Bereich Erpressungssoftware[48]. Der Cyber-Angriff auf die Seitensprungplattform Ashley Madison und die daraus resultierende Publikation von intimen Informationen führte zu einer Anzahl von Erpressungsversuchen. Kriminelle drohten damit, Details von außerehelichen Beziehungen öffentlich zu machen und verlangten Geld für ihr Stillschweigen[49]. Statt Geld hätten sie jedoch auch politische Ziele verfolgen können[50].

Ein gezieltes Eindringen in das Gerät eines:einer Politiker:in oder seiner:ihrer Familie kann den Zugriff auf Informationen ermöglichen, die im Falle der Veröffentlichung dem:der Politiker:in, seiner:ihrer Wahlkampagne, seiner:ihrer Partei oder der ganzen Regierung schaden. Dasselbe Szenario lässt sich für die Administratoren von IT-Systemen, die für Wahlen relevant sind, etwa Wahlmaschinen, durchspielen. Die Sorge über politische Cyber-Angriffe dieser Art wuchs nach dem Bekanntwerden russischer Angriffe auf Ziele in den USA[51] und im Vereinigten Königreich[52] im vergangenen Jahr sprunghaft an. Die mit Erpressung erzielten Auswirkungen können mit erheblicher Verzögerung zum Tragen kommen.

Angriffstaktiken	**Auswirkungen**	**Primäres Schutzziel Confidentiality, Integrity and/or Availability of Data**
Verfügbarkeit einschränken	Unmittelbar	Verfügbarkeit *Sekundär: Integrität*
Schwächung des Vertrauens	Unmittelbar	Integrität *Sekundär: Vertraulichkeit*
Manipulation	Unmittelbar und Mittelbar	Integrität
Ausspähung	Mittelbar	Vertraulichkeit *Sekundär: Integrität*
„Leaks“	Mittelbar	Vertraulichkeit *Sekundär: Integrität*
Persuasion	Mittelbar	Vertraulichkeit
Erpressung	Mittelbar	Vertraulichkeit

Tabelle 1. Angriffstaktiken auf Wahlen mit CIA Trias

48 Lily Hay Newman, The Ransomware That Hobbled Atlanta Will Strike Again

49 Alex Hern, Spouses of Ashley Madison users targeted with blackmail letters

50 Natasha Bertrand, Hacked Text Messages allegedly sent by Paul Manafort's daughter discuss 'bloody money' and killings, and a Ukrainian Lawyer wants him to explain

51 Kenneth P Vogel, David Stern and Josh Meyer, Manafort faced blackmail attempt, hacks suggest

52 Ben Riley-Smith, Blackmail fears after Parliament hit by 'sustained and determined' cyber attack on MPs' email network

Datenintensive Wahlen

Die strategischen Motivationen werfen ein Schlaglicht auf die allgemeinen Gründe für versuchte Einflussnahmen auf Wahlen. Die verwendeten Taktiken demonstrieren demgegenüber, wie die Angreifer:innen sich Schwachstellen der Datenintensiven Wahlen zu Nutze machen. Das Kapitel über die Taktiken zeigte anhand von Beispielen, wie Daten beschafft und für die Beeinflussung einer Wahl ausgenutzt wurden oder werden könnten. Bislang war von Daten im allgemeinen Sinn die Rede. Im Folgenden stellen wir nun das gesamte Spektrum der im Verlauf einer Wahl anfallenden Daten vor, um so die verschiedenen Angriffspunkte exakter klassifizieren zu können. Daten haben eine Schlüsselrolle für demokratische Wahlen. Politische Parteien setzen mehr und mehr auf digitale Werkzeuge, um Daten für ihre Kampagnen aufzubereiten, spezielle Technologien unterstützen den Prozess der Stimmabgabe[53], die Auszählung der abgegebenen Stimmen und die Prüfung der Wahlberechtigung der erschienenen Wähler:innen[54]. Es wird davon ausgegangen, dass viele Daten nicht exklusiv für die Wahl erhoben wurden, sondern auch in anderen gesellschaftlichen Zusammenhängen Verbreitung finden. Das bedeutet letztlich nichts anderes als: nicht alle Daten sind gleich. Daher wird in diesem Abschnitt analysiert, welche Daten während eines Wahlverfahrens eine Rolle spielen und wofür sie genutzt werden. Dabei wird auch differenziert zwischen Daten, die öffentlich verfügbar sind und solchen, die nicht öffentlich sind, analog zur CIA Trias. Dies ist ein analytisches Instrument, um zu sehen für welche Art von Missbrauch sich unterschiedliche Arten von Daten anbieten und welche Gegenmaßnahmen gegen den Missbrauch möglich sind.

Öffentlich zugängliche Wahldaten

Öffentlich zugängliche Daten im Rahmen einer Wahl sind Informationen, die im Zug einer Wahl und speziell als Teil der Wahl entstehen oder genutzt werden. In manchen Ländern schließt dies neben Wahlergebnissen, und tabellarischer Aufstellungen der Wahlergebnisse für statistische Zwecke auch Information über frühere Kandidat:innen, Statistiken über die Parteizugehörigkeit der Wähler:innen und Informationen über die Ausgaben für den Wahlkampf ein[55]. Daten über Wähler:innen kommen auch zum Einsatz, zum

53 Nicole Perlroth et al, Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny

54 Shannon Vavra, There's more than one way to hack an election

55 Es wird vermutet, dass russische Hacker während der 2016 Wahlbeeinflussung Informationen von einer Spendendatenbank aus Tennessee gestolen haben. Berichtet von Eric Geller, 60 Minutes DHS Election Security Report – Teil 1 und Teil 2.

Beispiel bei der digitalisierten Einteilung der Wahlbezirke (z. Bsp. USA[56], Mexiko oder Indien[57]). Diese Einteilung bedient sich unter anderem der Zensus Daten, allgemeiner Bevölkerungsdaten, Karten und manchmal Daten über frühere Wahlentscheidungen von Wähler:innen. Ein weiteres Beispiel für öffentlich zugängliche Daten sind jegliche Informationen und Medieninhalte, die Webseiten präsentiert werden, die in irgendeiner Weise mit der Wahl in Zusammenhang stehen. Dazu gehören etwa Webseiten mit den Parteiprogrammen oder Informationen auf den Seiten der lokalen Wahlbüros. Diese Art von Daten wurde bereits mehrfach Ziel von Cyber-Angriffen. Bei einer der Vorwahlen in den USA wurde ein DDoS-Angriff gegen die offizielle Webseite von Knox County in Tennessee durchgeführt. Das offizielle Wahlergebnis konnte so nicht abgefragt werden. Später wurde entdeckt, dass die DDoS-Attacke lediglich ein Ablenkungsmanöver war. Die Angreifer zielten gleichzeitig auf die Webserver Software[58], durch deren Kompromittierung man sich Zugriff auf ein breiteres Spektrum an Daten erhoffte. Ein weiteres Beispiel ist der Angriff auf die offizielle Webseite zur Wahl von Lee County in Florida. Auf der gehackten Seite erschien eine vulgärsprachliche Anti-ISIS Botschaft[59]. In Venezuela schickte ein Hacker angeblich Screenshots an das Wahlkampfteam des Präsidentschaftskandidaten Hugo Chavez, die belegten, dass er die Webseite von Chavez nach Belieben an- und ausschalten konnte[60]. All diese Angriffe richten sich gegen die Verfügbarkeit öffentlicher Informationen zur Wahl.

Öffentlich zugängliche Daten über die Wähler:innen finden sich an vielen verschiedenen Stellen (bei akademischen Institutionen, Behörden[61], Unternehmen, die Hochrechnungen und Prognosen erstellen, Medien, Hosting Anbietern, Nicht-Regierungsorganisationen[62]). Vertraulichkeit gehört hier oft nicht zu den Designprinzipien, vielmehr steht die Transparenz des Wahlverfahrens im Zentrum. Der ungehinderte Zugang und die Richtigkeit der Daten bleibt aber das Hauptschutzziel. Wenn Informationen über das Wahlprogramm eines:einer Politikers:Politikerin, einer Partei oder Information über die Wahl als solches nicht mehr zugänglich ist, kann dadurch der freiheit-

56 Ace Project, 1990 Census of Population And Housing P.L. 94-171 Redistricting Data

57 Ace Project, Electoral districts for greater accountability

58 Zaid Shoorbajee, Election day website crash in Knox County coincided with more direct hack, report says

59 Dave Elias, Update left Lee County Elections Website vulnerable to hackers

60 Tim Maurer and Agustin Rossi, Why Latin America Needs to Prepare Now for Election Meddling

61 Federal Election Commission, Contributions to All Candidates

62 Center for Responsive Politics, Follow The Money, A Handbook

liche Charakter und die Fairness einer Wahl beeinträchtigt werden. Manipulationen öffentlich zugänglicher Daten über eine Wahl können überdies deren Wahrnehmung durch die Bürgerschaft verändern und der Verbreitung von Fake News Vorschub leisten. Also ist es besonders wichtig, die Integrität und Zugänglichkeit der Daten zu schützen.

Personenbezogene Daten

Personenbezogene Daten sind Informationen über ein Individuum. Sie beziehen sich auf eine eindeutig identifizierte oder identifizierbare natürliche Person[63]. Wahlkampfteams und Regierungen sammeln große Mengen personenbezogener Daten von Wählern:Wählerinnen. Diese Daten können Angreifer:innen missbrauchen. Ergebnis von Cyber-Angriffen können Identitätsdiebstahl oder auch gezielt an bestimmte Personen gerichtete Desinformation über die Wahl, Kandidat:innen, politische Parteien oder wichtige Wahlthemen sein[64]. Persönliche Daten spielen im gesamten Verlauf einer Wahl eine Rolle. Bei der Wähler:innenregistrierung werden zur Identifikation beispielsweise Adresse, Geburtsdatum, Geschlecht und Augenfarbe erfasst. Andere Informationen wie Email Adressen sind kein geeignetes Merkmal zur Identifizierung, können aber dazu dienen, den:die Wähler:in zu erreichen. Parteien nutzen diese Art von personenbezogenen Daten für einen gezielteren Wahlkampf. Auch die Information über das Einkommen und die Religionszugehörigkeit kann dabei eine Rolle spielen. Selbst das Auto, das ein:e Wähler:in fährt, wird heute als mögliches Indiz für die Präferenz einer bestimmten Partei betrachtet. Während diese Daten auf den ersten Blick wenig mit der Wahl zu tun haben, dienen sie als wichtiges Kriterium für die Entscheidung der Parteien, welche Wähler:innen sie gezielt ansprechen[65]. Darüber hinaus hat der Einsatz biometrischer Daten zur Wähler:innenidentifizierung zugenommen[66]. 35 von 130 untersuchten Wahlkommissionen[67] weltweit erfassen bei der Registrierung der Wähler:innen biometrische Daten[68]. In Afrika und Lateinamerika werden biometrische Daten umfassend für die Identifikation

63 Es gibt unterschiedliche Definitionen, hier wird die Definition der Datenschutzgrundverordnung als weite Definition benutzt, siehe EUGDPR.org, GDPR FAQs What constitutes personal data

64 Darüber hinaus können diese Daten für Identitätsdiebstahl, zur Deanonymisierung und sogar für physische Angriff auf das Individuum (denn es handelt sich um persönliche Adressen) ausgenutzt werden.

65 Max Biederbeck, Chris Köver, Dirk Peitz, German Angstwahl: Die digitale Nervosität der deutschen Parteien

66 International IDEA, ICTS in Elections Database

67 Andauerndes Forschungsvorhaben International IDEA ICTS in Elections Database

68 International IDEA, ICTS in Elections Database

von Personen eingesetzt[69]. Der Diebstahl von Email Adressen in mehreren lateinamerikanischen Ländern und der anschließende Versand massenhafter Emails mit falschen Informationen über einen Wahlkandidaten, lieferte ein gutes Beispiel für den möglichen Missbrauch personenbezogener Daten[70]. Hat ein Angreifer ausreichend Informationen über eine Person, kann er sich überdies als diese Person ausgeben. Er kann damit beispielsweise die im Wählerverzeichnis[71] über den Wähler gespeicherten Daten ändern oder den Wahlvorgang behindern, indem er eine neue Briefwahladresse[72] angibt. Ein anderes Szenario ist der Eingriff in die Verfügbarkeit der notwendigen Daten am Wahltag. Damit kann die Ausübung des Wahlrechts behindert werden. Werden viele Bürger:innen auf diese Weise an der Stimmabgabe gehindert – und wird der Vorfall öffentlich – führt dies wiederum zu einem Vertrauensverlust in die Legitimität der Wahl.

Personenbezogene Daten sind nicht zwangsläufig öffentliche Informationen. Sie können aber durch Bürger selbst öffentlich oder zumindest zu anderen Personen und Gruppen zugänglich gemacht werden (zum Beispiel durch Angaben der Bürger selbst in öffentlichen Foren oder durch Emails) und ebenso durch die öffentliche Verwaltung oder private Firmen. Einige US-Staaten, etwa Florida[73], erlauben die Nutzung einiger personenbezogener Daten ihrer Bürger:innen und in Deutschland können Unternehmen mit eingeschränktem Umfang legal über die Einwohnermeldeämter auf diese Daten zugreifen[74]. Die Integrität der personenbezogenen Daten ist vor allem dort bedeutsam, wo ihre Manipulation zum Ausschluss von der Wahl führen kann. Angriffe auf die Verfügbarkeit der Daten scheint nicht zum Arsenal von Angriffstaktiken zu gehören. Die Vertraulichkeit ist als solche manchmal durch die breite Zugänglichkeit zu personenbezogenen Daten kritisch.

69 International IDEA, ICTS in Elections Database

70 Tim Maurer and Agustin Rossi, Why Latin America Needs to Prepare Now for Election Meddling

71 Latanya Sweeney, Ji Su Yoo, and Jinyan Zang, Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections

72 Minister des Innern und für Sport Hessen, Unique incidents in Hessen, Germany

73 Laut Section 97.0585, Florida Statutes, werden Wählerregistrierugsdaten, Führerscheinnummern von Florida Bewohnern oder ID Nummern aus Florida von einer Veröffentlichung ausgeschlossen. Die einschlägige Bestimmung ist die Section 1.3 der behördlich ausgestellten Daten.

74 Datenschutzbeauftragter-info, Meldedaten: Wie der Staat mit uns Geld macht

Selbstangaben

Selbstangaben sind im Unterschied zu personenbezogenen Daten, Informationen, die Bürger:innen selbst über sich angeben oder die Unternehmen aus deren Online Verhalten ableiten (so genannter ‚nutzergenerierter' Inhalt). Es müssen keine korrekten, nachgewiesenen oder die Person identifizierenden Daten sein, auch darin unterscheiden sie sich von personenbezogenen Daten. Zu dieser Kategorie von Daten gehören etwa biographische Angaben in Profilen Sozialer Medien, öffentlich zugängliche Nachrichten des einzelnen, sowie Charakterzüge oder Meinungen, die sich aus der Aktivität in Sozialen Netzwerken, aus Kaufhistorien[75] oder auch aus Nutzungsverhalten und dem daran geknüpften Tracking ergeben. Auch Parteien fragen intern solche Daten ab. Die FDP hat beispielsweise eine Software im Einsatz, mit der sie die Meinung der eigenen Parteimitglieder:innen zu bestimmten politischen Themen abfragen kann[76]. Dies kann auch anonym sein. Ein anderes Beispiel für die Nutzung von selbst angegebenen Daten lieferte die CDU, die mit der App Connect17 versuchte, Einblick in ihre potentielle Wähler:innenbasis zu gewinnen[77]. Selbstangaben sind grundsätzlich Nutzer:innen-generierte Inhalte und von Unternehmen zum Erstellen von Profilen durch das Tracking von Nutzern:Nutzerinnen gesammelte Informationen.

Die entstandenen Nutzer:innenprofile werden an Wahlwerbefirmen verkauft, die auf Basis der Informationen versuchen, die öffentliche Meinung und das Wahlverhalten zu formen. Auch Angreifer können jedoch in den Besitz der Daten gelangen, und sie dazu ausnutzen, um durch Polarisierung und das Anheizen gesellschaftlicher Kontroversen die öffentliche Meinung und das Wahlverhalten zu verzerren. Entsprechende Vorfälle waren sowohl in den USA[78] als auch in der EU[79] in der Vergangenheit bereits zu beobachten. Dabei ist die Integrität dieser Daten von großer Bedeutung für Parteien und Politiker:innen. Sie können helfen, die herrschende Meinung der Wählerschaft

75 Die gezogenen Schlüsse über Verhalten einer Person online, müssen nicht korrekt sein, da sie auf Algorithmen beruhen. Abgesehen von wenig exakt arbeitenden Algorithmen können auch veraltete, nicht schlüssige oder bewusst falsche Daten die Ergebnisse verzerren.

76 FDP Bundespartei, Meine Freiheit

77 Christlich Demokratische Union Deutschlands (CDU), Connect 17 App

78 Facebook, Case Study: Reaching Voters with Facebook Ads (Vote No on 8) und Politico Staff, The social media ads Russia wanted Americans to see und Adam Entous, Craig Timberg and Elizabeth Dwoskin, Russian Operatives used Facebook to Exploit racial and religious divisions

79 Kaan Sahin, Germany Confronts Russian Hybrid Warfare and Tim Maurer and Agustin Rossi, Why Latin America Needs to Prepare Now for Election Meddling

besser zu verstehen (interne Umfragen), und können damit als Entscheidungsgrundlage für die Entwicklung politischer Strategien dienen[80].

Selbstangaben von Wähler:innen sind in der Regel nur zum Teil öffentlich, etwa in Form von bestimmten Bereichen von Profilen in Sozialen Medien. Die meisten der von zum Beispiel Facebook gehaltenen Daten sind jedoch nicht öffentlich (Tracking Information zur Bewegung von Nutzer:innen im Web, Informationen zu Ortsangaben, Daten zu Anrufen und Nachrichten[81]). Der Zugriff für eine Auswertung durch werbetreibende Unternehmen wird von Facebook vermarktet. Die von Nutzer:innen selbst angegebenen Informationen sind in erster Linie in der Hand von Marketing Unternehmen oder den einschlägigen Sozialen Medien, aber auch öffentliche Wahlforschungsunternehmen halten kleinere Bestände. Die Daten werden entweder von den entsprechenden Unternehmen selbst oder über spezialisierte Data Broker vermarktet, die sich die Daten aus verschiedensten Quellen beschaffen[82].

Die Verfügbarkeit ist nicht das höchste Schutzziel dieses Datentyps, denn Nutzer:innen können die Informationen jederzeit selbst reproduzieren oder Umfragen können durch Backups leicht gesichert werden. Kritisch ist die Integrität. Werden Informationen, wie Meinungen auf einer der Öffentlichkeit zugänglichen Plattform manipuliert, kann dies einen Verlust an Ansehen und politischen Schaden bedeuten. Auch die Manipulation von internen Umfragen kann kritisch sein, wenn darauf basierend Entscheidungen getroffen werden. Vertraulichkeit kann dann eine Rolle spielen, wenn die gemachten Angaben sensitiver Natur waren (z. Bsp. politische Präferenzen) und auf ein Individuum zurückzuführen sind (z. Bsp. Tracking Informationen über das Nutzungsverhalten im Netz).

Angriffe auf die Integrität von selbst gemachten Angaben der Nutzer:innen stellen sicherlich eine Bedrohung dar. Je mehr Parteien und lokale Regierungen auf diese Art von Informationen setzen, um politische Entscheidungen zu treffen, desto höher ist das Bedrohungspotenzial. Aktuell stellt die Kompromittierung der Vertraulichkeit mittels Tracking und Profiling der Nutzer:innen und der anschließende Verkauf dieser Daten sowie die Einschränkung bei der Sicherheit allerdings das größte Problem dar. Die Sicherheitslücken

80 Great Battlefield Podcast, Modernizing Technology and Security at the DNC, Raffi Krikorian, Chief Technology Officer of the DNC, diskutiert die Nutzung von Wählerinformationen und die Zukunft davon ab Minute 26.

81 Sean Gallagher, Facebook scraped call, text message data for years from Android phones

82 FTC, USA example of companies that hold consumer data
Bestimmte Datenschutzbestimmungen limitieren den Zugang oder die Nutzung von Daten.

beim Umgang mit den Daten[83] sind ein Risiko hinsichtlich der Vertraulichkeit. Zu den notwendigen Gegenmaßnahmen gehören nicht nur Verbesserungen in der Informationssicherheit und der Resilienz der Gesellschaft. Auch Datenschutzmechanismen wie Datensparsamkeit, Zustimmungsregelungen (Consent) und Zugriffsbeschränkungen sind unverzichtbar.

Von Behörden ausgestellte Daten

Behördlich ausgestellte Daten sind Informationen, die von Regierungen selbst über das Individuum ausgestellt werden. Beispiele sind der Führerschein, Sozialversicherungsnummern, Steuernummern, Pass- oder Personalausweisnummern. Im Rahmen der Wahl, wird dieser Datentyp im Wesentlichen zur Identifizierung und Authentifizierung der Wahlberechtigten bei der Wahlregistrierung (in Ländern, wo Bürger:innen sich aktiv registrieren müssen) oder bei der Stimmabgabe herangezogen. Die Wählerregistrierung ist beispielsweise in den USA komplett digital, allerdings gelten unterschiedliche Wahlidentifikationen und Registrierungsgesetze in den einzelnen Bundesstaaten.

Einige Bundesstaaten verlangen keinerlei Identifikation für die Registrierung, etwa Kalifornien. In anderen Staaten, etwa Alabama, müssen Bürger:innen Namen und Geburtsdatum angeben und von Behörden ausgestellte Identifikationsnachweise, etwa Führerscheine oder von den Bundesstaaten ausgegebene Identifikationsnachweise[84] vorlegen, um sich als Wähler:in eintragen zu lassen. Freiwillige Wahlhelfer:innen überprüfen dann mittels spezieller E-Books unter Verwendung der entsprechenden Datenbanken die Identität und stellen sicher, dass ein:e Wähler:in nur eine Stimme abgibt. In anderen Ländern werden Wahlberechtigte mittels ihrer Ausweise identifiziert, etwa in Deutschland. In Estland hat die Regierung spezielle Identifikationsnachweise für alle Bürger ausgegeben. Die estnische digitale eID dient einerseits zur Identifikation der Bürger:innen, andererseits ermöglicht sie digitale Signaturen. Mit dieser eID können estnische Wahlberechtigte online früher

83 Dell Cameron and Kate Conger, 2017 GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters

84 Latanya Sweeney, Ji Su Yoo, and Jinyan Zang, Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections

wählen. Etwa 30 Prozent der estnischen Wähler:innen griffen zuletzt auf diese Möglichkeit zurück[85].

Die von Behörden zur Identifizierung und für andere Zwecke ausgestellten Daten und dabei zugewiesenen Identifikationsnachweise sind in der Regel nicht öffentlich. Trotzdem können nicht nur die Bürger:innen und Behörden selbst, sondern, im Rahmen unterschiedlicher Verwendungszwecke, auch private Unternehmen von Steuerberatern über private Gefängnisse bis zu Hotels oder Fitness Studios auf diese Daten zugreifen[86]. Je weniger Verwendungszwecke es für die von den Behörden für Wahlen und zu Authentifizierungszwecken von Wählern erhobenen Daten gibt, desto geringer ist das Risiko, dass sie weit verbreitet sind. Wird ein Zugriff für alle möglichen Zwecke zugelassen, kann dies in Kombination mit anderen Datenquellen, wie dem Zugriff auf personenbezogene Daten und für Sicherheitszwecke erhobene Daten, zu Identitätsdiebstahl führen und die Manipulation einer Wahl begünstigen, indem Angreifer:innen sich Zugang zu entsprechenden Datenbanken verschaffen und etwa Anschriften von Wähler:innen verändern. Die Risiken und Kosten eines solcher Angriffe wurden in den USA bereits untersucht[87]. Von der Regierung ausgestellte Daten müssen verfügbar, und valide sein und sind dabei so vertraulich wie möglich zu behandeln – alle drei „Schutzziele“ sind also für diese Kategorie von Daten einschlägig.

Vertrauliche Kommunikation

Bei vertraulicher Kommunikation handelt es sich um Informationen, die zwischen mindestens zwei Kommunikationspartnern:partnerinnen ausgetauscht wurden, innerhalb oder außerhalb einer Gruppe (Partei, Wahlkampfteam, Abwicklung eines Geschäfts). Die Erwartung ist, dass diese Informationen nicht an Dritte weitergegeben werden, also nicht öffentlich sind. Würde die Information dennoch öffentlich, wäre damit möglicherweise ein Schaden für das Ansehen, den Status oder die Integrität eines der involvierten Mitglieder:innen oder der gesamten Gruppe verbunden. Das konkrete Risiko besteht darin, dass private Kommunikation enthüllt wird, die eine Kandidatur oder ein Wahlkampfteam belastet oder schlicht das Bild vermittelt, dass die Informationssicherheit einer für eine Wahl relevanten IT-Infrastruktur kompromittiert wurde – einschließlich der Infrastrukturen von Parteien oder Wahlkampfteams. Im US-Wahlkampf 2016 wurde private Kommunikation

85 E-Estonia, i-voting in Estonia; Valimized, statistics about Internet Voting in Estonia

86 Michael Link, Kommentar: Unerlaubte Ausweiskopien – niemanden kümmert‘s

87 Latanya Sweeney, Ji Su Yoo, and Jinyan Zang, Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections

enthüllt, die zeigte, dass Mitglieder des Democratic National Committee offensichtlich hinter den Kulissen klar Hillary Clinton unterstützten und sich gleichzeitig über die Kandidatur von Senator Bernie Sanders (Vermont) lustig machten[88].

Die allgemeine Erwartung geht zwar dahin, dass private Kommunikation vertraulich ist, tatsächlich haben aber auch andere Akteure oft Zugriff auf die entsprechenden Informationen. Es wurde zum Beispiel vermutet, dass Angestellte von Sozialen Medien wie Twitter auf Direktnachrichten[89] zugreifen. Dasselbe gilt für Textnachrichten, Emails und weitere private Kommunikation, sofern sie nicht Ende-zu-Ende verschlüsselt ist[90]. Überdies können solche Daten (z. B. Wahlkampfstrategien) auch bei den Agenturen gespeichert werden, die für die Unterstützung des Wahlkampfs von den Kandidaten:innen engagiert worden sind.

Die Verfügbarkeit und die Integrität dieser Daten sind kritisch. Das entscheidende Risiko im Zusammenhang mit privater Kommunikation bleibt jedoch unerwünschte Offenlegung und der Verlust der Vertraulichkeit.

Sicherheitsdaten

Sicherheitsdaten, wie zum Beispiel Nutzernamen und Passwörter dienen zur Absicherung von Systemen, die den Zugriff auf Daten, die für die Wahl relevant sind ermöglichen. Telefonnummern, etwa wenn sie für die Zwei-Faktor-Autorisierung[91] genutzt werden, ebenso wie der Fingerabdruck zum Entsperren des Smartphones, sind Teil dieses Datentyps. Im Wahlkampf sind Nutzernamen und Passwörter vor allem im Zusammenhang mit der Nutzung von Sozialen Medien von Interesse. Politiker:innen geben ihre Zugangsinformationen häufig an Mitarbeiter:innen weiter, damit diese ihre Kanäle in Sozialen Medien wie Instagram oder Twitter betreuen können. 2017 wurden die Passwörter für den Zugang von Konten in Sozialen Medien gestohlen und Hacker konnten damit auf die Twitter Konten von britischen Parlamentsabgeordneten zugreifen[92]. Gelingt es, Email-Konten oder Konten in Sozialen

88 Michael D. Shear and Matthew Rosenberg, Released Emails Suggest the D.N.C. Derided the Sanders Campaign

89 Catherine Shu, Twitter hits back again at claims that its employees monitor direct messages

90 Julia Löhr, Warum Jung von Matt Wahlkampf für die CDU macht

91 Wikipedia contributors. “Multi-factor authentication.”

92 Press Association, Russian hackers ‘traded stolen passwords of British MPs and public servants’

Medien zu übernehmen, können sie darüber andere Daten, auch vertrauliche Daten, manipulieren und falsche Informationen verbreiten, die dem Ansehen von Kandidat:innen und Wahlkampfteams schaden. Angreifer:innen könnten so auch unerkannt die Kommunikation beobachten und sich als Inhaber:in des Kontos ausgeben, um weitere Systeme oder Konten zu infiltrieren. Ein weiteres Angriffsszenario bei Wahlen ergibt sich dadurch, dass die Kombination von Nutzername und Passwort in manchen Staaten Zugang zu den Wahlmaschinen bietet. Mit einer solchen Kombination kann auch Änderungen in der Datenbank vorgenommen werden. Dies kann ihm:ihr erlauben, die Datenbank auf ein eigenes System zu kopieren, abgegebene Stimmen zu manipulieren und die Ergebnisse zurück ins offizielle System einzuschleusen[93]. Wahlmaschinen können auf diesem Wege auch unbrauchbar gemacht werden.

Sicherheitsdaten sollten naturgemäß immer nicht-öffentlich sein[94]. Im Idealfall sollte nur der:die Konto Inhaber:in über Zugangsdaten verfügen. Sie sollten mit keiner einzigen Person ausgetauscht werden. In den meisten Fällen ist für Passwortdaten ein Zurücksetzen, also die Erneuerung eines Passworts, möglich. Verfügbarkeit und Integrität spielen daher als Risikofaktoren eine untegeordnete Rolle. Der Schutz der Vertraulichkeit solcher Daten ist dagegen von größter Bedeutung.

93 Sam Thielman, Voting machine password hacks as easy as 'abcde', details Virginia state report und Jeremy Epstein, The Worst Voting Machine in America – Its password? "Admin."

94 Eine Ausnahme bildet die Zwei-Faktor-Authentifizierung, die neben dem Passwort zum Beispiel eine Email-Adresse oder Telefonnummer beinhaltet. Im Optimalfall sind beide Faktoren nicht öffentlich (bekannt).

Datentyp	**Rolle während der Wahl**	**Verbreitung**	***Schutzziel***
Öffentlich zugängliche Wahldaten	Wahlabschnitte zeichnen, Informationen über politische Akteure und die Wahl	Öffentlich	Verfügbarkeit, Integrität
Personenbezogene Daten	Wähler-authentifizierung, -registrierung, und Wahlakt	z.T. öffentlich *Zugänglich über öffentliche und private Akteure.*	Integrität Verfügbarkeit
Selbstangaben	Kampagnen, Umfragen	Teilweise öffentlich *Geteilt auf öffentlichen Plattformen mit privaten Akteuren und ggf. weit verbreitet.*	Integrität Vertraulichkeit
von Behörden ausgestellte Daten	Wähler-identifikation und -authentifizierung	Teilweise öffentlich *Geteilt mit Behörden, und Privatsektor*	Vertraulichkeit Integrität Verfügbarkeit
Vertrauliche Kommunikation	Kampagnen	Nicht öffentlich *Nur zugänglich für gezielte/bestimmte Gruppen/Personen*	Vertraulichkeit
Sicherheitsdaten	Kampagnen und wählen	Nicht öffentlich *Nur der Account Nutzer und ggf. Unternehmen, die Services bereitstellen wissen diese Informationen*	Vertraulichkeit

Tabelle 2. Datentypen in der datenintensiven Wahl

Schlussfolgerung

Die Beeinflussung der US-Wahl war ein Weckruf und ist bereits Gegenstand einer ganzen Reihe von Forschungsberichten und Analysen geworden[95]. Die Absicherung von Wahlen in der digitalisierten Welt erfordert eine erhöhte Aufmerksamkeit von Forschung, Politik und Gesellschaft. Wie wir über den Schutz von Wahlen nachdenken, ist wichtig. In der vorliegenden Analyse haben wir uns auf ein Grundelement der Digitalisierung konzentriert, die Datenbestände, auf die sie baut. Die identifizierten geopolitischen Motive und die Taktiken zur Ausnutzung von Daten, die für die Wahl relevant sind, legen nahe, dass der Schutz von Wahlen vor allem ein genaueres Verständnis über die Vertraulichkeit, Integrität und Verfügbarkeit von Daten, voraussetzt.

Auch wenn Angriffe auf die Integrität und die Verfügbarkeit langfristig nachwirken können, lassen sich beide mit den richtigen Maßnahmen oft wiederherstellen. Bei Angriffen auf die Vertraulichkeit verhält sich das etwas anders. Sind Daten wie private Kommunikation erst einmal veröffentlicht, kann die Vertraulichkeit nicht wiederhergestellt werden. Allen Fällen ist jedoch gemein, dass sie zu einem Verlust des Vertrauens der Bevölkerung in den demokratischen Prozess der Wahl führen können. Ein solcher Schaden an der Demokratie wäre schwer zu reparieren.

Angreifer:innen finden stets Wege zur Umgehung von Sicherheitsmaßnahmen. Ihre Strategie geht kann überdies auch dann aufgehen und einer Wahl nachhaltig Schaden zufügen, wenn die Kampagne nicht erfolgreich ist[96]. Angesichts dieser Beobachtungen kommen wir zu dem Schluss, dass Empfehlungen für die technische Absicherung der Daten, beispielsweise durch Mindeststandards für IT-Sicherheit bei Wahl-relevanten Systemen und Infrastrukturen, alleine nicht ausreichen. Von entscheidender Bedeutung ist auch die Resilienz der Gesellschaft.

95 Zum Beispiel Emefa Addo Agawu, How to Think About Election Cybersecurity: A Guide for Policymakers

96 Selbst wenn der Angriff nicht erfolgreich ist, bleibt er eine Bedrohung für die Wahl. Wie dargestellt, kann ein fehlgeschlagener Versuch der Beeinflussung trotzdem das Vertrauen in die Wahl erschüttern, sobald er öffentlich wird.
The Grugq, Campaign Information Security In Theory and Practice

Mehr Schutz für Wahlen: Empfehlungen und erprobte Praktiken

Die anschließende Liste von Empfehlungen und erprobten Praktiken in den Fußnoten zeigen Anwendungsbeispiele aus verschiedenen Ländern[97].

I. Grundlagen eines effektiven Schutzes für Wahlen

Regierungen sollten…

1. klar definieren, was national als Wahlbeeinflussung gilt und welche Systeme für die Wahl genutzt werden. Der Schutz von Wahlen muss als Prozess und dauerhafte Praxis verstanden werden.
2. den Schutz von Wahlen als Teil der nationalen Sicherheit verstehen (sowohl innenpolitisch, als auch außenpolitisch). Sie ist gemeinsam mit anderen Aspekten der nationalen Sicherheit zu diskutieren.[98]
3. den Schutz von Wahlen als gemeinsame Aufgabe von Behörden, privater und zivilgesellschaftlicher Partner:innen organisieren. Der Schutz ist gesamtgesellschaftlich zu betrachten.[99]
4. Mittel bereitstellen, die alle beteiligten Partner in die Lage versetzen, Sicherheit für die Wahlen zu gewährleisten. Es sind erhöhte finanzielle und personelle Mittel erforderlich.[100]
5. alle am Wahlprozess beteiligten Gruppen und Akteure eng einbeziehen und auf Sicherheitsfragen auf verschiedenen Ebenen aufmerksam ma-

97 Über weitere Beispiele würden sich die Autor:innen freuen. So kann die Liste sinnvoll erweitertet werden. Die angeführten Beispiele sollen exemplarisch mögliche Implementationen der Empfehlungen darstellen.

98 Beispiele:
Dustin Volz, Patricia Zengerle, Inability to audit U.S. elections a 'national security concern': Homeland Chief
Eric Brattberg and Tim Maurer, 2018 How Sweden Is Preparing For Russia to Hack its Election

99 Private Unternehmen sind für die Sicherheit von Wahlmaschinen und Lieferketten zuständig. Die Regierung ist für die Cyberabwehr verantwortlich. Zivilgesellschaft und Wissenschaft können ihre Expertise einbringen und als vertrauenswürdiger Akteur die Kommunikation unterstützen. Nur ein koordinierter Ansatz kann effektiv sein, um die Sicherheit der Wahlen zu erhöhen.

100 Beispiele:
Eric Brattberg and Tim Maurer, 2018 How Sweden Is Preparing For Russia to Hack its Election
The Times staff, 2018 Illinois finalizes its plans to prevent another hack
Morgan Chalfant, 2018 Senators introduce election security amendment to defense bill

chen. Wahlkampfteams, Parteien und Wahlbüros sollten dementsprechend unterstützt werden.[101]

II. Organisation

Regierungen sollten..

1. den permanenten Austausch und die Koordination zum Thema Sicherheit der Wahlen zwischen den Behörden (vertikal und horizontal) fest etablieren.[102]
2. eine Gruppe aus ressortübergreifenden Regierungsmitarbeiter:innen und Vertreter:innen von Nicht-Regierungsinstitutionen für den Informationsaustausch, die Entwicklung von Best Practices und die Koordination von Aktivitäten für die breitere Gesellschaft etablieren.[103]
3. vertrauenswürdige Partner:innen identifizieren, die gemeinsam mit der Privatwirtschaft, der Wissenschaft und der Zivilgesellschaft zu aktuellen Bedrohungen öffentlich kommunizieren können.[104]

III. Proaktive Sicherheitsmaßnahmen zum Schutz der Wahlinfrastruktur

Regierungen sollten...

1. eine fortlaufende Risikobewertungen für bei Wahlen eingesetzte Technologien etablieren. Der Prozess sollte unter anderem garantieren, dass eingesetzte Wahlsysteme dem aktuellen Stand der Technik entsprechen was IT-Sicherheit angeht. Ein nationales „Hack the Election"-Förderprogramm zum Aufspüren von Schwachstellen bei verwendeter Hardware,

101 Robby Mook Matt Rhoades Eric Rosenbach, 2017 Cybersecurity Campaign Playbook

102 Chris Bing, DNC pushes employees, campaigns to embrace email security habits ahead of midterms zitiert Raffi Krikorian, Chief Technology Officer im DNC: "Making the party secure and getting over the wounds of the hack of '16 is a cultural issue," he said. At the end of the day, "you can have the best technical defenses, but the weakest link could be your people. ... So culture change is probably one of the biggest things that we need to execute on."

103 Calvin Biesecker, DHS Creates Task Force To Bolster Election Security

104 Internationale Institutionen wie z. B. die OECD könnten weitere vertrauensvolle Akteure identifizieren.
Beispiele:
Mexikos Initiative "Verificado 2018": Andreas Rodriguez, Verificado 2018: Using collaborative journalism to fight fake news in Mexico
"Partnerschaft zwischen dem brasilianischem "Superior Electoral Court" und der "Brazil Computer Society" Angelica Mari, Brazilian government tries to prove e-voting is safe – A partnership with the Brazilian Computer Society aims at convincing the population that the electronic voting method is fraud-proof

Software und Online Diensten mit einer Verpflichtung diese zu schließen sollte implementiert werden.[105]

2. sicherstellen, dass die Beobachtung und Erkennung von gegen Wahlsysteme gerichtete Cyber-Angriffe ebenso wie Mechanismen um Betroffene im Ernstfall zu warnen etabliert werden[106]. Diese Mechanismen sollten in die regulären Prozesse zur Analyse von Sicherheitsproblemen in anderen Bereichen integriert werden[107].
3. eine Strategie festlegen, wie sie Cyber-Sicherheit über das gesamte Herstellungsverfahren von Wahl relevanter IT absichern können[108]. Sowohl beschaffte Software als auch Hardware, sowie Online Dienste sind dabei zu berücksichtigen. Die Strategie sollte Sicherheitsstandards, Berichtsroutinen und Zertifizierungsmechanismen umfassen.[109]
4. Unternehmen, die große Datenmengen von Bürger:innen/Wähler:innen verarbeiten, etwa Unternehmen die Soziale Medien betreiben, sind zur Datensparsamkeit anzuhalten.
5. den Wahlausgang durch Audits verpflichtend nachvollziehbar machen, um eine sichere und transparente Wahl zu garantieren. Für Forschung in diesem Bereich, sind finanzielle Mittel bereit zu stellen.
6. Sicherheitsprozeduren und Notfallmaßnahmen für den Ernstfall entwickeln, zum Beispiel durch die Identifikation von Bedrohungsszenarien und -modellen, sowie durch entsprechende Planspiele, um Administratoren:innen und für die Wahl wichtige strategische Akteur:innen fortzubilden.[110]

---

105 Matt Blaze et al, DEFCON 25 Voting Machine Hacking Village Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure
NIST, Voluntary Voting System Guidelines (VVSG) Recommendations to the EAC, August 31, 2007
Bundesamt für Sicherheit in der Informationstechnik Germany, Technical Guidelines

106 Falls dies keine Option ist, weil die Ressourcen fehlen, dann sollte zumindest der Zugang zu den Informationen sichergestellt werden, ggf. von einem anderen Land.

107 Beispiele einer Lageanalyse: Bundesamt für Sicherheit in der Informationstechnik, IT-Lagezentrum
Beispiele des Informationsaustauschs: Greenberg, The NSA confirms it: Russia hacked french election infrastructure

108 Wikipedia contributors, Supply chain cyber security

109 Eine Standardisierung des Prozesses könnte die Qualität der Lieferketten erhöhen. Es gibt bereits internationale Lieferketten Initiativen, diese müssten jedoch für Wahlsicherheit angepasst werden, NCSC, Guidance The principles of supply chain security
USA, Department of Homeland Security National Strategy for Global Supply Chain Security
Deutschland: Bundesministerium für Bildung und Forschung, Research for Civil Security Securing the Supply Chains

110 Schwedisches Civil Contingencies Agency (MSB), Jill Bederoff, Sweden is warned about foreign interference ahead of its election – and the country has 2 priorities to ward off attacks

IV. Fortbildung und Fähigkeitsentwicklung für Schlüsselakteure und die Öffentlichkeit

Regierungen sollten…

1. die Fähigkeitsentwicklung von Wahlkampfteams, Politiker:innen, Parteien und Ehepartner:innen hochrangiger Politiker:innen bei der IT-Sicherheit im Wahlumfeld fördern. Entsprechende Informationen und Expertise können von Behörden, Privatwirtschaft oder Nicht-Regierungsinstitutionen bereitstellen. Maßnahmen zu der Fortbildung und zur Vermittlung von Wissen können beispielsweise über das Bereitstellen von technischer Expertise erfolgen. So könnten freiwillige IT-Expert:innen den Betroffenen zur Seite gestellt oder Gelder für diesen Zweck zur Verfügung gestellt werden.[111]
2. einen kritischen Umgang mit Nachrichten – online und offline[112] – fördern, besonders im Kontext von Wahlen in Verbindung mit geopolitischen Entwicklungen. Diese Kompetenz sollte Teil der Lehrpläne werden[113].

V. Strategische Kommunikation für bessere Resilienz

Regierungen sollten…

1. proaktiv mit Medien und Wähler:innen über die Sicherheitsstrukturen der Wahl und der genutzten IT-Infrastrukturen kommunizieren. Dadurch kann das Vertrauen in die Wahl und die Fähigkeit diese zu schützen, gestärkt werden. Das Ziel muss sein, falschen Vorstellungen zu begegnen, mit Ängsten auszuräumen, die Transparenz zu verbessern und entgegen der „Praxis Security by Obscurity“ (Sicherheit durch Verschleierung) regelmäßig Informationen anzubieten, etwa bei der Wählerregistrierung

111 Beispiele:
Eine Idee könnte es sein, diese Art der Zertifizierung für Wahlsicherheitshelfer:innen auszubauen. BSI Certified IT Pen Testers, Bundesamt für Sicherheit in der Informationstechnik, Zertifizierung als Penetrationstester
Sicherheitscheckliste und Daten-Bootcamp der DNC, Chris Bing, DNC pushes employees, campaigns to embrace email security habits ahead of midterms

112 Kritischer Journalismus, genug Finanzierung und Bildung sind dabei Ansätze.

113 Hierbei können Estland, Finnland und Italien als Beispiele dienen:
Estland “ranks among the “best-equipped countries to resist the post-truth, fake news and their ramifications”, Open Society Institute Sofia, Common Sense Wanted: Resilience to ‘Post-Truth’ and its Predictors in the new Media Literacy Index 2018
Finnish Media Education, National Audiovisual Institute, Finnish Media Education Promoting Media and Information Literacy in Finland
Italiens Curriculum, NPR, Italy Takes Aim At Fake News With New Curriculum For High School Students; Jason Horowitz, In Italian Schools, Reading, Writing and Recognizing Fake News

(USA), im Rahmen des Versands von Wahlinformationen (Deutschland) oder bei anderen Gelegenheiten.

VI. Potentiale in der internationalen Kooperation bei Schutz von Wahlen nutzen

Regierungen sollten…

1. sicherstellen, dass Informationen, die eine Wahl bedrohen zwischen Geheimdiensten und unter befreundeten Staaten ausgetauscht werden[114].
2. eine internationale Datenbank mit eingeführten und erprobten Praktiken (“Best Practices) zur den besten Sicherheitskonzepten für Wahlen schaffen und pflegen und dabei positive und negative Erfahrungen aus der Umsetzung kontinuierlich aufnehmen.[115]
3. internationale Standards für sichere Technologien, die bei einer Wahl genutzt werden, entwickeln.
4. geschaffene internationalen Standards zum Schutz von Wahlen und erprobte Praktiken in Trainingsverfahren in die internationale Entwicklungsarbeit integrieren.

114 “Establish a G7 Rapid Response Mechanism to strengthen our coordination to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for coordinated response”, G7, CHARLEVOIX COMMITMENT ON DEFENDING DEMOCRACY FROM FOREIGN THREATS

115 Beispiele internationaler Netzwerke, wo Informationen geteilt werden: Brazil Superior Election Court, Cooperation with International Organizations

Annex A: Angriffsvektoren

Ein Angriffsvektor (attack vector) ist ein von einem:einer Angreifer:in genutzter Weg, um sich Zugang zum System eines Ziels zu verschaffen[116] und ist deswegen Grundlage jeder Angriffstaktik. Die folgenden Abschnitte liefern einen Überblick über die gebräuchlichsten Angriffsvektoren, die genutzt werden, um ein bestimmtes Ziel zu erreichen.

Ausnutzung von Software Schwachstellen

Elektronische Geräte laufen mit Software. Das gilt für das individuell genutzte Smartphone ebenso wie für Server von Online Diensten (zum Beispiel Email Dienste oder Soziale Medien). Software hat, vor allem mit zunehmender Komplexität, Schwachstellen. Eine Schwachstelle ist eine Sicherheitslücke, oder auch ein Fehler im Programm, die ein:e Angreifer:in ausnutzen kann und somit Zugang zum System erhält[117]. Ein:e Angreifer:in programmiert in der Regel Schadsoftware, oder passt sie, um eine entsprechende Schwachstelle ausnutzen. Schwachstellen bleiben Nutzer:innen im normalen Betrieb meistens verborgen, was sie zu einem idealen Angriffsvektor macht. Die meisten im folgenden beschriebenen Angriffsvektoren basieren in der einen oder anderen Weise auf Schwachstellen in der Software (oder Hardware). Schwachstellen können entweder per Fernzugriff oder lokal ausgenutzt werden, etwa durch die Verbindung des anzugreifenden Geräts mit einem mit Schadsoftware infizierten USB Datenträgers.

Angriff auf die Herstellungskette

Ein Angriff auf die Herstellungskette kann für Cyber-Angriffe auf Wahlen verwendet werden[118]. Ein:e Angreifer:in versucht dabei die Systeme eines Herstellers zu kompromittieren, etwa eines Herstellers für Wahlmaschinen. Sollte ihm:ihr das Gelingen, könnte er:sie das zum Beispiel das nächste Software Update verändern. Sobald es dann ausgerollt wird, werden alle Wahlmaschinen, die aktuell im Einsatz sind, mit dem kompromittierten Update versorgt. Auf diesem Weg könnten der Wahlausgang manipuliert oder die Wahlmaschinen auf verschiedenste Art unbrauchbar gemacht werden.

116 ISACA, Attack Vector Definition, 2018

117 Oscar Celestino Angelo Abendan II, Gateways to Infection: Exploiting Software Vulnerabilities

118 Institute for Critical Infrastructure Technology, The Painfully Vulnerable Election System and Rampant Security Theater

Spear Phishing

Spear Phishing ist ein Betrugsversuch, bei dem der Angreifer:in sein:ihr Opfer davon zu überzeugen versucht, dass die Kommunikation von einer vertrauenswürdigen Quelle kommt um so zum Beispiel an bestimmte Daten zu kommen. Die vertrauenswürdige Quelle, hinter der sich tatsächlich der:die Angreifer:in verbirgt, kann der eigene Email Anbieter, ein:e Kollege:Kollegin, ein:e Freund:in oder eine vertrauenswürdige Institution sein. Solche Angriffe zielen in erster Linie darauf ab, Zugang zum System des Opfers zu bekommen, etwa zum Email Konto oder zur Infrastruktur des jeweiligen Arbeitgebers, indem das Opfer unbewusst Information über das eigene Konto an den:die Angreifer:in übermittelt. Der:die Angreifer:in kann eine solche Übermittlung auch durch das Einbringen von Schadsoftware in das System des Opfers forcieren[119]. Eine beliebte Variante des Spear Phishing besteht darin, Hyperlinks in einer Email zu versenden, um das Opfer damit auf eine vom:von der Angreifer:in kontrollierte Seite zu locken, oder dem Opfer mit Schadsoftware versehene Anhänge zu senden. Beispielsweise könnte eine infizierte politische Studie zu einem aktuellen Ereignis als Vorwand übersandt werden.

Angriff von innen

Das Szenario des „Insider Angriffs“ beschreibt das Risiko, dass ein:e böswilliger:böswillige Akteur:in sich in eine Institution einschleicht (oder dort schon arbeitet) und von dort aus den Angriff verursacht (dies schließt ehemalige Angestellte oder Vertragsnehmer ein, deren Zugangskennungen noch nicht widerrufen wurden). Auch Herstellerketten können betroffen sein. Der Insider kann Zugriff auf wichtige Dokumente und Daten haben, Sicherheitsprozeduren kennen oder, im schlimmsten Fall, sogar mit Administratorrechten für die gesamte IT-Infrastruktur ausgestattet sein. Der Zugang solcher Angreifer:innen und die Möglichkeit, ihre Spuren vollständig zu verwischen, macht diese Angriffsmethode sehr gefährlich und kann zu nachhaltigem Schaden führen[120].

Whaling

Whaling ist eine individualisiertere Form des Spear Phishing und nutzt die gleichen Techniken, konzentriert sich dabei aber auf „die großen Fische“,

119 Faris Azimullah and Anu Nayar, Spear Phishing 101: What is it and how to avoid it?

120 Marcell Gogan, Insider Threats as the Main Security Threat in 2017

Topmanager:innen hochrangige Politiker:innen oder Regierungsmitglieder. Die extreme Personalisierung der Angriffe erschwert deren Aufdeckung erheblich[121].

Waterholing

Dieser Angriff beginnt mit dem sorgfältigen Auskundschaften des Ziels, bei der ein:e Angreifer:in etwa beobachtet, welche Webseiten von den beabsichtigten Zielen häufig aufgesucht werden. Im nächsten Schritt wird der:die Angreifer:in zunächst versuchen, solche Webseiten zu unterwandern, um dort Schadcode einzuspeisen. Dies erlaubt dem:der Angreifer:in schließlich den Rechner des Opfers beim Besuch dieser sonst vertrauenswürdigen Webseite zu infizieren[122].

Social Engineering

Social Engineering Angriffe erfordern typischerweise eine Form der psychologischen Manipulation der Zielperson. Beliebt ist beispielsweise die Vorspiegelung einer Situation, die Eile gebietet oder Angst oder ähnliche Emotionen provoziert und das Opfer damit dazu veranlasst, ohne weiteres Nachdenken sensible Informationen wie Passwörter preiszugeben, auf mit Schadcode unterlegte Links zu klicken[123] oder ein entsprechend infiziertes Dokument zu öffnen.

Spoofing

Unter Spoofing versteht man eine Angriffsmethode, bei der ein:e böswilliger:böswillige Akteur:in sich als jemand anderes oder als ein anderes Gerät ausgibt, um Identitäts- oder Sicherheitschecks zu unterlaufen oder um sein Opfer über seine Identität zu täuschen[124]. Spoofing ist nicht nur ein technischer Angriffvektor. Es kann auch als Social Engineering Variante auftreten. Ein:e Angreifer:in kann beispielsweise eine Webseite, Email-Adresse, oder Online Identität so abändern, dass sie einer vertrauenswürdigen Quelle ähnlich ist und damit das Opfer täuschen.

121 Nena Giandomenico, What is a whaling attack? Defining and Identifying whaling attacks

122 Oscar Celestino Angelo Abendan II, Watering hole 101

123 Nate Lord, Social engineering attacks: Common techniques & how to prevent an attack

124 Veracode, Spoofing attack: IP, DNS & ARP

Man-in-the-Middle Angriff (MITM)

Bei diesem Angriffvektor konzentriert sich der:die Angreifer:in darauf Mittelsmann zwischen dem:der Nutzer:in auf der einen Seite und dem besuchten Server oder der benutzen Anwendung auf der anderen Seite zu werden. Eine beliebte Variante dieser Methode besteht zum Beispiel darin, einen unsicheren Router zu übernehmen, der etwa für den Zugang zum WLAN an einem Flughafen oder in einem Kaffee genutzt wird. Sobald der:die Angreifer:in einen solchen Router übernommen hat, kann er die Online Aktivitäten der Nutzer:innen, die sich über den Router anmelden, ausspähen, die Inhalte der Kommunikation verändern und Schadsoftware auf den Rechner einer Zielperson aufspielen[125], um ihn damit für künftige Angriffe vorzubereiten[126].

(Distributed) Denial of Service Attacke (DDoS)

Ein (Distributed) Denial of Service Angriff ist ein Angriffsvektor, bei der ein:e Angreifer:in das Überschwemmen eines Systems mit Anfragen von verschiedenen Systemen aus organisiert. Die entstehende Überlast macht den Server oder die Anwendung, auf den es der:die Angreifer:in abgesehen hat, für Dritte unerreichbar[127]. Nutzer:innen können Informationen oder Dienste, die das überlastete System anbietet, damit nicht mehr in Anspruch nehmen.

125 Symantec, What is a man in the middle attack?

126 Serge Malenkovich, Was ist eine Man-in-the-Middle-Attacke?

127 Akamai, (Distributed) denial-of-service Attack

Über die Stiftung Neue Verantwortung

Cyber-Sicherheitspolitik wird zunehmend ein elementares Feld nationaler und internationaler Politik. Hierzu gehören unter anderem die institutionelle Aufstellung, die Ressourcenlage und -verteilung, Prozesse und rechtliche Rahmenbedingungen, sowie die Auswirkungen nationaler Politik auf die internationalen Beziehungen ("Spillover-Effekte").

Auch wenn vieler dieser Herausforderungen subsidiär auf nationaler Ebene begegnet werden muss, so ist es zwingend notwendig international voneinander zu lernen und zusammen gute Lösungen, sogenannte Best Practices, zu entwickeln und diese weiterzuverbreiten. Zu diesem Zweck wurde das Transatlantic Cyber Forum, kurz: "TCF", von der Stiftung Neue Verantwortung gegründet.

Das TCF besteht derzeit aus mehr als 100 amerikanischen, deutschen und weiteren EU-Expert:innen, welche in Zivilgesellschaft, Wissenschaft und Privatwirtschaft tätig sind.

Das Transatlantic Cyber Forum wird von der Robert Bosch Stiftung und der William and Flora Hewlett Foundation gefördert.

Über die Autoren

Sven Herpig ist Leiter des Transatlantic Cyber Forums (TCF) und bringt dort die Expert:innen von beiden Seiten des Atlantiks zu allen Facetten der Innen-, Sicherheits- und Verteidigungspolitik im Cyber-Raum zusammen.

Julia Schuetze ist Projektmanagerin des Transatlantischen Cyber Forums und beschäftigt sich in diesem Zusammenhang mit internationaler Cybersicherheitspolitik.

So erreichen Sie die Autoren

Dr. Sven Herpig
Projektleiter Internationale
Cyber-Sicherheitspolitik
sherpig@stiftung-nv.de
+49 (0)30 81 45 03 78 91

Julia Schuetze, M.A.
Projektmanagerin
Transatlantic Cyber Forum
jschuetze@stiftung-nv.de
+49 (0)30 81 45 03 78 82

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de