Deutscher Bundestag
Ausschuss für die Angelegenheiten der Europäischen Union
Ausschussdrucksache
19(21)86
Anhörung 2. März 2020

Sachverständigenstellungnahme von Julia Schuetze, Projektmanagerin für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für die Sitzung des Bundestagsausschusses für die Angelegenheiten der Europäischen Union am 02.03.2020 zum Thema "Wehrhaftigkeit der demokratischen Verfasstheit der EU und Integrität von Willensbildungsprozessen"

Die folgende Stellungnahme bezieht sich vor allem auf die Drucksache 19/9225 (Schutz der liberalen Demokratie in Europa" vom 09.04.2019), und Fragenkatalog vom 11. 02. 2020 zur Öffentlichen Anhörung zur Wehrhaftigkeit der demokratischen Verfasstheit der EU und Integrität von Willensbildungsprozessen[1], aber auch auf die aktuellen Gesetzes- und Policy-Entwicklungen innerhalb der Bundesregierung, wie dem IT-Sicherheitsgesetz 2.0, und der Europäischen Union, wie der NIS-Richtlinie, dem “Blueprint for European coordinated response to large-scale cybersecurity incidents and crises” und der Cyber Diplomacy Toolbox. In meiner Stellungnahme gehe ich spezifisch auf die Cybersicherheit[2] von Wahlen ein. Ich stütze mich bei meiner Stellungnahme vor allem auf die Ergebnisse der Analyse “Der Schutz von Wahlen in vernetzten Gesellschaften”[3], veröffentlicht 2018 gemeinsam mit Herrn Dr. Herpig und auf meine Arbeit zur europäischen Cybersicherheitspolitik und Cyberaußenpolitik im Rahmen des von der Europäischen Kommission finanzierten Forschungsprojekts EU Cyber Direct[4].

In meiner Stellungnahme möchte ich Ihnen vor allem aufzeigen,

1. dass auch Daten, die nicht unmittelbar mit demokratischen Prozessen in Verbindung stehen, für Angriffe missbraucht werden können (z.B. personenbezogene Daten, private Kommunikation). Die potentielle Angriffsoberfläche ist deshalb größer als zunächst ersichtlich[5].
2. dass Angreifer:innen verschiedene Motivationen haben können, z.B. Delegitimierung des demokratischen Prozesses, Schwächung des Vertrauens in die Demokratie, Diskreditierung von Akteuren. Diese Motivation kann Aufschluss über die Ziele bzw. weiteres Vorgehen der Angreifer:innen geben.
3. dass bei Cyberangriffen die Möglichkeit, dass es sich nicht um einen Angriff von außen handelt, zu selten in Betracht gezogen wird. Mögliche "Innentäter:innen" könnten so übersehen werden.
4. dass ein Cyberangriff nicht unbedingt erfolgreich sein muss, um das Vertrauen in den demokratischen Prozess zu erodieren. Die Wahrnehmung solcher versuchten Angriffe wird stark durch die Kommunikation darüber beeinflusst.

Maßnahmen zum Schutz von Wahlen haben zwei Schwerpunkte: Verbesserte Cybersicherheit von Wahlen und der gemeinsame EU-weite Umgang mit Cyberangriffen auf Wahlen.

1. Es muss ermittelt werden, welche Daten und Systeme kritisch für eine Wahl sind und gleichermaßen, wie die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und Systemen im Sinne der IT-Sicherheit geschützt werden kann. Dies muss als Prozess und dauerhafte Praxis betrachtet wird. Alle am Wahlprozess beteiligten Gruppen und Akteure sollten eng zusammenarbeiten und auf Sicherheitsfragen aufmerksam gemacht werden. Wahlkampfteams, Parteien und Wahlbüros sollten dahingehend unterstützt werden.

---

[1] Spezifisch auf Fragen eins, zwei, drei, vier, elf und 14

[2] „Cybersicherheit ist breiter angelegt als IT-Sicherheit und umfasst zusätzlich auch sozio-kulturelle, politische, rechtliche und weitere Dimensionen.“ Sven Herpig, Anti-War and the Cyber Triangle.

[3] Sven Herpig und Julia Schuetze, Der Schutz von Wahlen in vernetzten Gesellschaften Wie sich die Sicherheit datenintensiver Wahlen erhöhen lässt.

[4] EU Cyber Direct - Supporting EU Cyber Diplomacy

[5] Siehe Sven Herpig und Julia Schuetze, Der Schutz von Wahlen in vernetzten Gesellschaften Wie sich die Sicherheit datenintensiver Wahlen erhöhen lässt. “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”.

2. Für den Umgang mit Cyberangriffen auf Wahlen innerhalb der EU, sollte die Bundesregierung evaluieren, wie Deutschland reagieren würde, welche Informationen mit welchen Akteuren geteilt werden müssen, unter welchen Umständen gemeinsam reagiert wird und welche Maßnahmen im Rahmen einer gemeinsamen Reaktion eingesetzt werden können. Diese Antworten sind wichtig, um die Operationalisierung der Cyber Diplomacy Toolbox gemeinsam mit anderen Mitgliedstaaten und den EU Institutionen zu gestalten. Das Simulieren verschiedener Szenarien kann dabei unterstützen.

Das Problem erläutert: Angriffstrategien und konkrete Fallbeispiele

Durch Cyber-Angriffe kann Zweifel daran gesäet werden, dass eine Wahl korrekt und nachvollziehbar abgehalten wurde, was den demokratischen Prozess delegitimieren könnte. Dabei müssen die entsprechenden Angriffe nicht notgedrungen erfolgreich sein. Die Wahrnehmung, dass IT-Systeme und Wahl-Infrastruktur angreifbar oder manipulierbar sind, kann dem demokratischen Prozess seine Legitimation (in der Öffentlichkeit) entziehen. Es reicht, dass die Wähler:innenschaft glaubt, dass das Wahlergebnis nicht den „Willen des Volkes“ widerspiegelt. Sowohl in den USA[6] als auch in Deutschland[7] gibt es Beispiele vor oder nach einer Wahl, wo Kandidat:innen Wahl- oder Umfrageergebnisse öffentlich via soziale Medien anzweifeln und von Wahlfälschung sprechen. Die Glaubwürdigkeit solcher Aussagen würde natürlich dadurch erhöht werden, dass in dem Zeitraum Cyberangriffe auf die Wahlinfrastruktur nachweislich stattgefunden haben.

A) *Das Vertrauen in den demokratischen Prozess* als solchen kann durch einen Angriff auch dann untergraben werden, wenn kein einzelner politischer Akteur von dem Angriff profitiert. Es reicht, dass der Angriff öffentlich bekannt wird, um die Legitimität des Prozesses zu untergraben. Diese Taktik zielt im Wesentlichen auf die Integrität der für die Wahl notwendigen Daten und die öffentliche Wahrnehmung der Sicherheit der Wahlen ab. Die öffentlichen Aufdeckung von Schwachstellen bei Wähler:innenverzeichnissen, oder bei Software zur Stimmauszählung[8] sind Beispiele. Ein Vertrauensverlust gegenüber der Wahl ist eine mögliche Konsequenz dieser Angriffstaktik. Der Schaden kann unabhängig davon eintreten, ob die Manipulation aufgedeckt und behoben wird. Die Schwachstellen müssen dafür auch nicht zwangsläufig ausgenutzt werden.

Solche Schwachstellen zu finden und schließen ist von größter Bedeutung, eine Veröffentlichung sollte allerdings in einem geordneten Verfahren und gemäß den Maßgaben etablierter Richtlinien (Coordinated Vulnerability Disclosure) zur Bekanntgabe von Schwachstellen – inklusive entsprechender Kommunikationsmaßnahmen – erfolgen.

Beispielfälle

Im Vorfeld der deutschen Wahlen 2017 gelang es Hacker:innen, Schwachstellen in der Software für die Zusammenführung und Übertragung von Auszählungsergebnissen aufzuzeigen[9]. Diese wird von Mitarbeiter:innen der Wahlleiter:innen verwendet, um die vorläufigen Ergebnisse einzugeben, auszuwerten und schnell an die jeweils nächsthöhere Wahlbehörde zu übermitteln. Bisher liegt die Entscheidung darüber, welche Wahlsoftware eingesetzt wird bei den verschiedenen Akteuren, zum Beispiel könnten die Gemeindewahlleitung, die Kreiswahlleitung, die Landeswahlleitung und die Bundeswahlleitung verschiedene Software einsetzen. Dies führt dazu, dass es einen Flickenteppich[10]

[6] The Independent (2020) Trump calls Fox 'fake news' for citing unfavourable 2020 election polls & BBC (2016) Trump: 'I'm afraid the election's going to be rigged'

[7] ZDF (2020). AfD-Abgeordneter Brandner -Mutmaßung über Wahlfälschung

[8] Biermann & Stark (2017) Die Bundestagswahl kann manipuliert werden

[9] 46halbe (2017), Software zur Auswertung der Bundestagswahl unsicher und angreifbar

[10] Locker und Mützel (2017) Flickenteppich Wahlsoftware: Diese Karte zeigt, wer am Sonntag welches Programm einsetzt und Eckert (2017) Wahlsoftware in Deutschland vor EU-Wahl: Intransparent, unkontrolliert – und möglicherweise manipulierbar

an eingesetzter Software gibt. Es bestehen außerdem keinerlei Mindeststandards oder Updatepflichten. Vor der Wahl konnte das Bundesamt für Sicherheit in der Informationstechnik die Behebung der Sicherheitslücken der betroffenen Software zwar begleiten und Empfehlungen aussprechen[11], aber es besteht keine gesetzliche Verpflichtung für den Hersteller diese umzusetzen bzw. für die zuständigen Akteure nur Software einzusetzen, die zertifiziert ist.

Im Präsidentschaftswahlkampf in den USA 2016 haben Angreifer:innen relevante Systeme[12] in 50 Bundesstaaten auf Schwachstellen getestet und dabei Akteure, die für die Administration der Wahl zuständig sind, anvisiert[13]. Diese Taktik der Ausspähung hat vor allem vertrauliche Daten zum Ziel und etwaige Angriffe versuchen, Systeme zu infiltrieren, um sie später von innen zu überwachen und möglicherweise Daten auszuleiten. Ein Nebeneffekt ist die Verletzung der Integrität des Systems, indem etwa der heimliche Zugriff auf Daten über eine so genannte Backdoor ermöglicht wird. Ein weiterer Folgeeffekt des Ausspähungstaktik 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.

B) *Die Diskreditierung politischer Akteure* wie Politiker:innen, Parteien, Interessensgruppen oder der aktuellen Regierung kann ein Werkzeug sein, um die öffentliche Meinung zu beeinflussen, und somit ein bestimmtes Wahlergebnis zu forcieren.

Die einfachste Möglichkeit, um politische Akteure zu diskreditieren ist die Verbreitung von Informationen oder Dokumenten, die politische Akteur:innen in einem schlechten Licht erscheinen lassen. Solches Material kann durch Cyberangriffe beschafft werden und dann öffentlich gemacht werden (“Leaken”). In Verbindung mit einer auf eine bestimmte Zielgruppe ausgerichteten Ansprache und Adressierung (zum Beispiel durch Micro-Targeting) kann dafür gesorgt werden, dass mit relativ geringem finanziellen und personellen Aufwand ein hoher Schaden angerichtet wird. Dieser besteht in diesem Szenario darin, gezielt Wähler:innen von einer bestimmten politischen Position zu überzeugen. Die Manipulation 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. Es ist auch möglich, dass Angreifer:innen die erlangten Informationen einer dritten Partei zuspielen, um die Intentionen der Angreifer:innen zu verschleiern und möglicherweise zugleich die Glaubwürdigkeit des gestohlenen Materials zu erhöhen.

Die Angriffsmöglichkeiten bei dieser sogenannten Persuasion (Überzeugung) sind breit gefächert, die Auswirkungen können beträchtlich sein, weil sich Persuasion mit vielen anderen Strategien der Wahlbeeinflussung verbinden lässt. 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 Gesellschaft, die über die Möglichkeiten dieser Beeinflussung aufgeklärt ist und deshalb resilient darauf reagieren kann .

<u>Beispielfälle</u>

[11] BSI (2017) BSI-Stellungnahme zu Wahlsoftware

[12] Mascaro & Jalonick (2019) Senate report: all 50 states were targeted by Russian interference ahead of 2016 elections “Senate Intelligence committee concluded all 50 states were targeted in 2016 and ahead of the 2018 election “top election vulnerabilities remained.”

[13] Mueller (2019) Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Page 50 “In addition to targeting individuals involved in the Clinton Campaign, GRU officers also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities. The GRU also targeted private technology firms responsible for manufacturing and administering election-related
software and hardware, such as voter registration software and electronic polling stations.”

Der Fall von Emmanuel Macrons „En Marche!"-Partei hat gezeigt, dass gestohlene Daten zusätzlich auch gezielt manipuliert werden können, um größtmöglichen Schaden anzurichten[14]. Hier zeigte sich, dass strategische Kommunikation in einem solchen Fall unabdingbar ist. Macrons Partei hat unmittelbar nach dem Angriff ein Statement herausgegeben, welches den Hack bestätigte, aber darauf hinwies, dass unter den geleakten Dokumenten auch Fälschungen sind, die für Desinformationskampagnen und zur Verunsicherung der Wähler:innenschaft genutzt werden könnten.

Der erfolgreiche Cyberangriff[15] auf das Democratic National Committee (DNC), fand weltweit große Beachtung, als im US Präsidentschaftswahlkampf 2016 die zeitlich klug platzierte Veröffentlichungen der 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[16].

Welche Rolle personenbezogene Daten Daten spielen, zeigt ein Fall aus Kolumbien, wo ein Hacker Datenbanken mit Email-Adressen hackte, die dann im Wahlkampf für den Versand von Emails mit falschen Informationen über einen Wahlkandidaten missbraucht wurden[17]. Dies liefert ein gutes Beispiel für den möglichen Missbrauch personenbezogener Daten in Kombination mit einer Disinformationskampagne.

C) Durch die Taktik der Einschränkung der Verfügbarkeit von wahlrelevanten Informationen, kann auch der *Meinungsbildungsprozess beeinflusst oder eine Schwächung des Vertrauen* erzeugt werden.

Webseiten, Soziale Medien, Email-Konten, Kurznachrichtendienste und IT-Infrastrukturen sind wichtige Mittel, um den Wähler:innen Informationen zur Verfügung zu stellen. Ein:e potentielle:r 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. Eine solche 'Einschränkung der Verfügbarkeit' kann sich gegen politische Parteien, Kandidat:innen oder auch gegen die öffentliche IT-Infrastruktur der Politik allgemein richten, beispielsweise Systeme und Netzwerke, die Informationen für die Wahl
bereithalten. Wenn Informationen über das Wahlprogramm eines:einer Politiker:in, einer Partei oder Information über die Wahl selbst nicht mehr zugänglich ist, kann dadurch der freiheitliche 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.

Beispielfälle

Der entsprechende Effekt der Nicht-Verfügbarkeit von wahlrelevanten Informationen 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[18]. Die beiden Seiten waren 2012 von fast der Hälfte aller niederländischen Wähler:innen genutzt worden, um sich für eine:n der Kandidat:innen zu entscheiden[19].
Ein weiteres Beispiel ist auch ein DDoS-Angriff auf Computersysteme in Knox County, Tennessee. Die offiziellen Vorwahlergebnisse mehrerer lokaler Wahlen, die für den 1. Mai 2018 angekündigt waren,

[14] Nossiter (2017) Hackers Came, but the French Were Prepared

[15] Geller (2019) Collusion aside, Mueller found abundant evidence of Russian election plot

[16] Dovere (2016) Heads roll at the DNC

[17] Robertson (2016) How to Hack an Election Andrés Sepúlveda rigged elections throughout Latin America for almost a decade. He tells his story for the first time.

[18] Van Riper (2017) Turk Hack Team and the "Netherlands Operation"

[19] Reuters (2017) Dutch voting guide sites offline in apparent cyber attack

konnte so nicht abgefragt werden[20]. Später wurde entdeckt, dass der DDoS-Angriff lediglich ein Ablenkungsmanöver war, denn die Angreifer:innen zielten gleichzeitig auf die Software[21] des Webservers, durch deren Kompromittierung man sich Zugriff auf ein breiteres Spektrum an Daten erhoffte.

In Schweden wurde im Rahmen der Parlamentswahlen 2018 durch Denial of Service Attacks die Verfügbarkeit von der Webseite der Sozialdemokraten kurzzeitig eingeschränkt[22]. Weitere Angriffe auf Twitter-Accounts der Partei wurden auch nach der Wahl festgestellt[23].

Maßnahmen zum Schutz von Wahlen

A) Die Umsetzung der folgenden Maßnahmen zielen vor allem darauf ab, wahlrelevante Systeme und Daten vor Cyberangriffen zukünftig besser zu schützen

Durch die Entwicklung von Angriffstaktiken und der Digitalisierung des Abstimmungsprozesses[24] in der EU, braucht es eine fortlaufende transparente Risikoanalyse und Bewertung, welche Technologien für den Wahlprozess geeignet sind und welche nicht. Während in Deutschland eine entsprechende Entscheidung des Bundesverfassungsgerichts zum Beispiel den Einsatz von Wahlcomputern für verfassungswidrig erklärt hat, gibt es in anderen EU-Ländern keine entsprechenden Entscheidungen[25]. Es gibt bisher keinen Gesamtüberblick in Deutschland oder EU-weit, der beschreibt, welche Systeme für eine Wahl genutzt werden und welche Sicherheitsnieveau diese haben. Im Rahmen der Evaluierung der NIS Richtlinie[26] und des IT-Sicherheitsgesetz 2.0, sollte die Bundesregierung darauf hinwirken, dass für eine Wahl relevante Systeme besondere Schutzmaßnahmen unterliegen und Risikoanalysen bekommen.

Ein nationales „Hack Election Technology“-Förderprogramm zum Aufspüren von Schwachstellen bei verwendeter Hardware, Software und Online-Diensten, wie zum Beispiel auf der DefCon in den USA[27], sollte implementiert werden. Allerdings sollte es mit einer Verpflichtung, gefundene Schwachstellen zu schließen, aufgesetzt werden.

Vor der EU Wahl 2019 wurde ein Kompendium für die Cybersicherheit von Wahl- Technologien veröffentlicht[28], wo durch Beispiele aus verschiedenen Mitgliedsstaaten so genannte “Best Practices” gezeigt wurden. Das Kompendium sollte in eine Datenbank eingepflegt werden und mit internationalen

---

20 Dorman (2018) Cyberattack crashes Knox County election website; votes unaffected

21 Shorbarjee (2018) Election day website crash in Knox County coincided with more direct hack, report says

22 Swedish Security Services (2018) Attempts to influence confidence in the election process & The Local (2018) Sweden's Social Democrats' website hacked in attack linked to Russia and North Korea

23 BBC (2019) Swedish Social Democrats' Twitter account hacked & Heyman (2019) Sweden’s largest party investigating messages sent during Twitter hack

24 zum Beispiel gibt es Bestrebungen in Bulgarien elektronische Wahlen einzuführen siehe The Sofia Globe (2019) Bulgarian MPs amend Electoral Code to neuter preferential vote, expand machine voting “As regards electronic voting, which Parliament legislated in 2016, the amendments required the Central Electoral Commission to draft a road map for its introduction by March 31 2020”.

25 BVerfGE 123, 39 - Wahlcomputer “Beim Einsatz von elektronischen Wahlgeräten müssen die wesentlichen Schritte von Wahlhandlung und Ergebnisermittlung zuverlässig und ohne besondere Sachkenntnis überprüft werden können. Die Notwendigkeit einer solchen Kontrolle ergibt sich nicht zuletzt im Hinblick auf die Manipulierbarkeit und Fehleranfälligkeit elektronischer Wahlgeräte. Bei diesen beruht die EntgeBVerfGE 123, 39 (71)BVerfGE 123, 39 (72)gennahme der Wählerstimmen und die Berechnung des Wahlergebnisses auf einem Rechenvorgang, der von außen und für Personen ohne informationstechnische Spezialkenntnisse nicht überprüfbar ist.”

26 European Commission (2020) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Commission Work Programme 2020

27 Beuth (2017) 100 Sekunden, um einen Wahlcomputer zu hacken

28 NIS Cooperation Group (2018) Compendium on Cyber Security of Election Technology CG Publication 03/2018

Beispielen stetig erweitert werden, um dabei positive und negative Erfahrungen aus der Praxis einzupflegen und kontinuierlich aufzunehmen.

Die von Macron angestrebte Agentur zum Schutz europäischer Demokratien könnte diese Maßnahmen personell und koordinierend unterstützen und den Gesamtüberblick behalten, und Verknüpfungen von Cyberangriffen mit Desinformationskampagnen herstellen. Die Agentur sollte allerdings mit etablierten Akteuren für die IT-Sicherheit in Europa, der European Union Agency for Cybersecurity, und relevanten Akteuren, wie dem BSI in Deutschland und weiteren in den Mitgliedsstaaten zusammenarbeiten. Maßnahmen müssen gemeinsam und koordiniert umgesetzt werden.

Die Fähigkeitsentwicklung, z.B. das Erkennen von Phishing-Emails oder das Nutzen von Zwei-Faktor-Authentifizierung, muss in Wahlkampfteams, bei Politiker:innen, Parteien und Ehepartner:innen hochrangiger Politiker:innen dringend gefördert werden. Es sollten Mittel bereitgestellt werden, die alle beteiligten Akteure in die Lage versetzen, IT-Infrastrukturen zu schützen und entsprechende Trainings zu durchlaufen.

Proaktiv mit Medien und Wähler:innen über die Sicherheitsstrukturen der Wahl und der genutzten IT-Infrastrukturen kommunizieren, ist wichtig, um das Vertrauen in die Wahl und die Fähigkeit, diese zu schützen, zu stärken. Das Ziel muss sein, falschen Vorstellungen zu begegnen, Ängste auszuräumen, die Transparenz zu verbessern und entgegen der „Praxis Security by Obscurity“ (Sicherheit durch Verschleierung) regelmäßig Informationen anzubieten, etwa im Rahmen des Versands von Wahlinformationen (Deutschland) oder bei anderen Gelegenheiten. Dies kann zum Beispiel durch eine proaktive Informationkampagne über Wahlprozesse erfolgen, wie es in Schweden der Fall war[29].

B) Folgende Maßnahmen zielen vor allem darauf ab, wie Deutschland gemeinsam auf EU Ebene mit Cyberangriffen auf Wahlen umgehen kann.

Wie die Fallbeispiele zeigen, gab es schon einige Angriffe auf Wahlen innerhalb der EU. Es gibt erste Entwicklungen, um auf EU Ebene gemeinsame Reaktionen zu ermöglichen[30]. Dazu gehören Maßnahmen zur Mitigation, wie Koordinations- und Kooperationsmöglichkeiten als auch Maßnahmen im Kontext der Gemeinsamen Sicherheits- und Außenpolitik.
Der kontinuierliche Austausch von Informationen zur Analyse von Cyberangriffen ist wichtig, um zum Beispiel feststellen zu können, wenn ein Cyberangriff in einem EU Land dem eines anderen EU Landes ähnelt. Mechanismen zum Austausch dieser Informationen sollten für den Schutz von Wahlen dauerhaft genutzt werden, denn nur dann kann auch EU-weit eingeschätzt werden, wie und gegebenenfalls auch von welchen Akteuren die Demokratien in der EU bedroht sind. Dafür sollten Informationen spezifisch mit diesem Fokus geteilt und ausgewertet werden. Diese Analysen können die Grundlage für zukünftige EU-weite politische und strategische Entscheidungen zum Schutz von Wahlen bilden.

Bezogen auf Maßnahmen in Reaktion auf Cyberangriffe, die zur Gemeinsamen Sicherheits- und Außenpolitik fallen, wie in der EU Cyber Diplomacy Toolbox[31] vorgesehen. Ist es wichtig zu verdeutlichen, dass diese momentan nur eingesetzt werden können, wenn alle Mitgliedstaaten zustimmen. Deswegen ist es besonders wichtig, dass sich Mitgliedstaaten darüber im Klaren werden,

---

[29] Swedish Security Services (2018) Attempts to influence confidence in the election process “In the run-up to the elections, the Security Service has dedicated extensive resources to information, education and cooperation in order to increase awareness of the fact that influence operations aiming to damage public confidence in the election process and our democratic system may happen.”

[30] European Commission (2019) A Europe that protects: good progress on tackling hybrid threats & Council of the EU (2019) Cyber-attacks: Council is now able to impose sanctions & European Commission (2017) Blueprint für European coordinated response to large-scale cybersecurity incidents and crises

[31] Council of the European Union (2017) Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities

was sie selbst in Reaktion auf Cyberangriffe auf Wahlen machen würden. Die Bundesregierung sollte parallel zur Operationalisierung der Diplomacy Toolbox diskutieren, unter welchen Umständen sie gemeinsam mit anderen Staaten reagieren würde, welche Instrumente eingesetzt werden können und welche Informationen es für die Umsetzung von Maßnahmen braucht. Die Bundesregierung sollte sich außerdem aktiv am Prozess der Operationalisierung beteiligen und sich in dem Rahmen mit anderen Mitgliedstaaten über deren Herangehensweise austauschen. Die Operationalisierung der Diplomacy Toolbox ist ein Prozess, an dem sich Mitgliedstaaten aktiv beteiligen, um so die Anwendung von bestimmten Maßnahmen zu diskutieren oder zu erproben und dann zu evaluieren. Das Simulieren verschiedener Fälle kann dabei unterstützen.

Fazit

Cyberangriffe auf Wahlen dienen verschiedenen Zielen, zum Beispiel das Vertrauen in den demokratischen Prozess als solchen zu erodieren, bestimmte Akteure zu diskreditieren oder die Verfügbarkeit von Informationen, die für die Meinungsbildung relevant sind, einzuschränken. Cyberangriffe dienen auch als Grundlage für Disinformationskampagnen. Um damit umzugehen müssen Cyberangriffe auf Wahlen durch die Verbesserung von Cybersicherheit der wahlrelevanten Systeme und Daten vereitelt werden. Des Weiteren sollte die Bundesregierung evaluieren, wie es mit erfolgreichen Cyberangriffen aus Wahlen innerhalb der EU umgehen würde und dabei entscheiden wie vorhandene Maßnahmen auf EU Ebene eingesetzt werden würden.