Mündliche Stellungnahme von Dr. Sven Herpig, Leiter Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, zur Cybersicherheitsstrategie 2021 im Nationalen Cyber-Sicherheitsrat am 15.06.2021

Liebe Damen und Herren,

Ich möchte mich erst einmal herzlich für die Einladung bedanken, heute hier sprechen zu dürfen.

Es gibt in der Strategie viele Maßnahmen, die zu befürworten sind, zum Beispiel die Absicherung von Maschinellem Lernen, die Stärkung des Bundes-Security-Operations-Center und der Mobile Incident Response Teams, die engere Verzahnung bei der Bund-Länder Kooperation, oder die Vorfallsbearbeitungsamtshilfe durch die Bundeswehr, aber auch die Weiterentwicklung und Zusammenarbeit bei der Cyber Diplomacy Toolbox auf EU-Ebene. Die **Einbeziehung der Zivilgesellschaft in Policy- und Gesetzgebungsvorhaben** im Bereich der Cybersicherheitspolitik ist, vor allem Dank Herrn Staatssekretär Richter, besser geworden, hat aber noch Luft nach oben. Das ist aber sicherlich etwas für ein bilaterales Gespräch.

Der Bereich des Controllings ist nach eigener Angabe noch nicht ganz fertig, aber die Leitlinie “Ziele messbar und transparent ausgestalten” ist ein guter Anfang. Er führt aber nicht weit genug. Es braucht eine unabhängige Evaluierung, die nicht vom federführenden Ressort der Strategie beauftragt wird. Weiterhin braucht es positive und/ oder negative Anreize für die Umsetzung der Maßnahmen und Erreichung oder Nicht-Erreichung der Ziele. Behörden könnten so zum Beispiel Planstellen für die Umsetzung von Maßnahmen bekommen oder die verantwortlichen Behördenleiter:innen sollten sich bei Nicht-Erreichung dem Innenausschuss im Parlament stellen müssen.

Die Cybersicherheitsarchitektur wird in der Strategie an mehreren Punkten adressiert. So heißt es zum Beispiel: “Aber auch die staatliche Cybersicherheitsarchitektur ist auf den Prüfstand zu stellen und zeitgemäß fortzuentwickeln”. Dort wird die engere Verzahnung der Akteure auf Bund- und Länderebene angesprochen. Jedoch sollte darüber hinaus die Cybersicherheitsstrategie des Bundes mit denen der Länder abgestimmt werden. Analog zur

Abstimmung der deutschen Cybersicherheitsstrategie mit der Cybersicherheitsstrategie der Europäischen Union.
Ich rege aber darüber hinausgehend an, dass die Bundesregierung den Mut haben muss bestehende Plattformen, Behörden und Gremien zu reformieren oder abzuschaffen, wenn das notwendig sein sollte. So müsste zum Beispiel das Gremium in dem wir uns hier befinden grundlegend reformiert werden, damit es seiner Rolle als strategisch-politisches Leitgremium in der Cybersicherheitsarchitektur gerecht werden kann. Ist diese Rolle nicht gewollt, muss man auch eine Abschaffung in Betracht ziehen.
Das Nationale Cyberabwehrzentrum sollte nicht nur stärker mit den Ländern, sondern auch mit der Industrie, verzahnt werden und ein Errichtungsgesetz erhalten. Letzteres gilt auch für die Zentrale Stelle für Informationstechnik im Sicherheitsbereich. Es kann nicht sein, dass trotz dem, in der vorliegenden Strategie geplanten, Ausbau von ZITiS und der jahrelangen Kontroverse um die Errichtung per Ministererlass kein Wort über ein Errichtungsgesetz verloren wird.

Die Evaluation der notwendigen Kompetenzen und Befugnisse der Sicherheitsbehörden im Cyberraum ist ein interessanter Aspekt. Die Strategie spricht hier davon, dass “[kontinuierlich zu überprüfen ist,] ob die staatlichen Institutionen über ausreichende Kompetenzen und Befugnisse verfügen [... und wenn] Regelungs- oder Fähigkeitslücken identifiziert werden, sind diese zu schließen”. Das ist leider nur teilweise richtig. Die Bundesregierung muss auch die bestehenden Kompetenzen und Befugnisse überprüfen und ineffektive Befugnisse streichen. Hierzu sollte man sich zum Beispiel die Grundrechtseinschränkungen anschauen, die mit der Quellen-TKÜ und Online-Durchsuchung einhergehen und sie in Relation zu den Verfahren setzen, wo sie erfolgreich eingesetzt worden sind und sonst nicht zugängliche, verwertbare Beweise geliefert haben.

Beim Schutz der kleinen und mittelständischen Unternehmen kommt die Strategie leider nicht wirklich über Informationsangebote hinaus.. Das hat die letzten Jahre nicht funktioniert und wird auch in Zukunft als alleinige Maßnahme nicht funktionieren. Hier braucht es konkrete Werkzeuge wie skalierbare Lösungen. Wie wäre es beispielsweise mit Public-Private-Partnerships für ein Schadsoftwareerkennungs- und Präventionssystem für KMUs? Für Behörden haben wir das.

Die Strategie nährt wieder einmal den Mythos von der Verbraucherin als Schwachstelle. Man wirft den Verbraucher:innen “digitale Sorglosigkeit” vor. Die

Verantwortung liegt nur zu einem kleinen Teil bei den Verbraucher:innen, und umso mehr bei den Herstellern, die ohne Sanktionen unsichere Produkte und Dienstleistungen auf den Markt bringen und betreiben dürfen. Wir brauchen klare Vorgaben für Hersteller statt Victim Blaming. Es ist an der Zeit, dass die Bundesregierung diesen Punkt versteht.

Die Förderung der IT-Sicherheitsforschung wird auch in der Strategie wieder als Allheilmittel tituliert. Natürlich ist es wichtig, dass zukünftig Maschinelles Lernen und Quantencomputer vernünftig abgesichert sind. Aber was genau ist denn aktuell die größte Gefährdung für Deutschland im Cyberraum? Vermutlich Cyberkriminalität im engeren Sinne und Wirtschaftsspionage. Was sind hier die bekannten Einfallstore? Nicht oder nicht korrekt umgesetzte, bekannte technische und organisatorische Maßnahmen. Entweder aufgrund von Fehlern oder von Risikoübernahmen. Die Basis für Informationssicherheit ist eine effektive und wirksame Umsetzung bewährter Sicherheitstechnologien – eine vertrauenswürdige IT-Infrastruktur ohne Hintertüren oder Ähnliches. Darüber will aber niemand reden, man flüchtet sich lieber in Forschungsförderung. Das geht am Problem vorbei.

Kommen wir zur Gefahrenabwehr. Unabhängig davon wie man dazu inhaltlich steht, hat sich die Bundesregierung dazu entschieden dieses Thema in der aktuellen Legislatur nicht weiterzuverfolgen, unter anderem weil es dazu möglicherweise eine Grundgesetzänderung bräuchte. Es ist daher unangebracht, wenn die aktuelle Bundesregierung der nächsten ins Aufgabenheft schreibt entsprechende Änderungen vorzunehmen, wenn sie sich selbst, sicherlich aus guten Gründen, entschieden hat das Thema nicht voranzutreiben.

Die Maßnahme zur Mandatierung von Hintertüren, oder wie es die Strategie nennt: “Entwicklung technischer und operativer Lösungen für den rechtmäßigen Zugang zu Inhalten aus verschlüsselter Kommunikation [...]”, gerade in einer Cyber**sicherheits**strategie, kann eigentlich nur als verspäteter Aprilscherz verstanden werden. Ich möchte an dieser Stelle an den Offenen Brief von Wirtschaft, Wissenschaft und Zivilgesellschaft vom 11. Juni 2019 erinnern, der die damaligen entsprechenden Pläne der Bundes- und Landesregierungen kritisierte. Innerhalb von einer Woche wurde dieser Brief von knapp 100 deutschen und europäischen Firmen und Organisationen unterzeichnet, dazu kamen über 150 Cybersicherheitsexpert:innen und Abgeordnete des deutschen Bundestags aus allen Fraktionen außerhalb der AfD und CDU/CSU. Mit der EU-Ratspräsidentschaft hat die Bundesregierung dieses Vorhaben jetzt auf die EU-Ebene getragen. Es wird ausländischen Nachrichtendiensten und Kriminellen mehr nutzen als unseren Sicherheitsbehörden und

gleichzeitig der europäischen IT-Wirtschaft stark zusetzen. Mal ganz abgesehen von der internationalen Signalwirkung und den Auswirkungen für besonders schutzbedürftige Bevölkerungsgruppen, die ein solches Vorhaben hätte. Die aktuelle Verfassungsschutzaffäre in Sachsen gibt hier einen ersten Einblick. Die Naivität der Deutschen Bundesregierung bei diesem Vorhaben ist erschreckend.

Komplett unverständlich ist, dass trotz allen Forderungen nach mehr Ressourcen und Ausweitungen von Befugnissen für Sicherheitsbehörden, nicht mit einem Wort der notwendige, gleichzeitige Ausbau von Schutz- und Kontrollmaßnahmen angesprochen wird. Ein Aspekt, der sogar im aktuellen Koalitionsvertrag zu finden ist. Deutlich wird diese gefährliche Asymmetrie wie bereits erwähnt zum Beispiel beim fehlenden Errichtungsgesetz für ZITiS. Aber auch bei der Ausweitung der nachrichtendienstlichen Vorfeldaufklärung, der Gefahrenabwehr oder dem Einbau von Hintertüren werden weder Schutzmaßnahmen noch Kontrollmechanismen auch nur mit einem Wort erwähnt..

Die Strategie vermischt in einem besorgniserregenden Umfang unter dem Begriff Cybersicherheit Maßnahmen die tatsächlich die IT-Sicherheit erhöhen können, mit Maßnahmen, die die IT-Sicherheit und Vertrauenswürdigkeit der IT-Infrastrukturen grundsätzlich gefährden, um Cyberkriminalität im weiteren Sinne und hybride Bedrohungen zu bekämpfen oder nachrichtendienstliche Überwachung durchzuführen. Dass es diese Begehrlichkeiten seitens der Sicherheitsbehörden gibt ist seit Jahren bekannt, umso verwunderlicher ist es, dass sie erst zu einem so späten Zeitpunkt in dem Entwurf der Cybersicherheitsstrategie zur Debatte gestellt werden – gerade so als wollte man in den letzten Monaten nicht darüber reden und hoffe, dass sie in der aktuellen Fassung untergehen würden.
Die Bundesregierung muss hier klar differenzieren und Maßnahmen, die die IT-Sicherheit schwächen aus der aktuellen Cybersicherheitsstrategie herausstreichen und sie dann in eine nationale Sicherheitsstrategie oder Ähnliches überführen – im aktuellen Entwurf vom 9. Juni 2021 betrifft das mindestens die Maßnahmen 8.3.1, 8.3.7, 8.3.8, 8.3.9, 8.3.11, 8.3.12, 8.3.14, 8.4.7..

Zusammenfassend mangelt es der Strategie an einigen wichtigen Stellen, wie den Anreizen für die Umsetzung, an Mut. Gleichzeitig fehlen elementare Aspekte wie der bessere Schutz von Politiker:innen und Parteien oder eine konkrete Vision für Resilienz und IT-Sicherheit, zum Beispiel in einem relevanten Bereich in dem Deutschland führend ist, wie industrielle Steueranlagen.

Das viel größere Problem ist jedoch, dass die Strategie durch eine Reihe an Maßnahmen zu einer Strategie der nationalen Sicherheit ohne zusätzliche Kontrollmechanismen verkommt, die möglicherweise der IT-Sicherheit in Deutschland mehr schadet als ihr nutzt.
Aus meiner Sicht ist die Cybersicherheitsstrategie 2021 in ihrer aktuellen Fassung für die Zivilgesellschaft untragbar. Da wir uns dem Ende dieser Legislaturperiode nähern, sollte die finale Verabschiedung und Implementierung der Cybersicherheitsstrategie der kommenden Bundesregierung überlassen werden; einer Bundesregierung der zum Beispiel der Minister des federführenden Ressorts ohnehin nicht mehr angehören wird. Das gebietet meine Erachtens die gute Regierungsführung.

OUTTAKE: Erfolge der Bundesregierung bei der IT- und Cybersicherheitspolitik würden sich in einer sinkenden Gefährdungslage widerspiegeln. Diese steigt aber laut den Lageberichten der IT-Sicherheit in Deutschland des Bundesamtes für Sicherheit in der Informationstechnik und den Bundeslagebildern Cybercrime des Bundeskriminalamtes stetig an oder stagniert zumindest auf hohem Niveau.

Das einzige Legislativvorhaben der Bundesregierung für die Stärkung der IT- und Cybersicherheitspolitik, das Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, hat sich über Jahre hingezogen und wurde dann in der Ausschussanhörung im Bundestag durch alle (!) geladenen Sachverständigen fundamental kritisiert. Die Kritik umfasste dabei fast alle Punkte des Vorhabens, vom Einsatz von kritischen Komponenten in Kritischen Infrastrukturen ("Lex Huawei") über das IT-Sicherheitskennzeichen bis hin zum Ausbau von Befugnissen im Sicherheitsbereich.

Auf der anderen Seite wurden mit der Novelle des BND-Gesetzes, der Harmonisierung des Verfassungsschutzrechts und der Bundespolizeigesetz-Novelle Legislativvorhaben verabschiedet, deren Befugniserweiterungen für Sicherheitsbehörden unter anderem durch den Einsatz von Schad- und Überwachungssoftware sowie des dafür benötigten Ökosystems (u. A. der Erwerb und das Vorhalten von Schwachstellen, Exploits und entsprechenden Werkzeugen und Plattformen) der IT- und Cybersicherheit in Deutschland eher schaden als nutzen werden. Die aktuelle Bundesregierung priorisiert Überwachung klar über IT-Sicherheit. Die

Cybersicherheitsstrategie bildet hier keine Ausnahme. Einen seit Jahren versprochenen ernsthaften Dialog mit Zivilgesellschaft und Industrie zu dem Thema gibt es bis heute nicht.