D02NEU Schluss mit ABCD-Waffen: A?chtung von Digitalwaffen.

Gremium:	Juso-Landesvorstand
Beschlussdatum:	09/28/2020
Tagesordnungspunkt:	0.D - Demokratie/Innen/Außen/Rüstung

Antragstext

Nie wieder Krieg durch Deutschland. Das gilt auch im Internet. Daher lehnen wir den Einsatz von digitalen Angriffswaffen konsequent, absolut und ohne Ausnahme ab. Digitale Angriffswaffen sind im Sinne einer Zusatzvereinbarung zum Genfer Protokoll weltweit zu ächten.

Der Einsatz und das Vorhalten digitaler Waffen durch staatliche wie private Institutionen muss strengstens untersagt und geahndet werden.

Digitale Angriffswaffen unterliegen im Vergleich zu bislang bekannten Kriegswaffen im Besonderen dem Risiko der Proliferation – der unbeabsichtigten Weitergabe an Dritte. So geschehen bei der Schadsoftware Wannacry, da digitale Angriffswerkzeuge ohne großen Aufwand vervielfältig werden können.

Defensive IT-Sicherheitsstrategie

Im digitalen Raum ist es erstmals theoretisch möglich, über rein defensive Maßnahmen vollständige Sicherheit für alle zu erzeugen. Jegliche digitale Angriffswerkzeuge gefährden im Gegensatz dazu immer die IT-Sicherheit für alle, da diese immer auf bewusst nicht geschlossenen Sicherheitslücken in IT-Systemen basieren, anstatt diese zu schließen. Wir fordern daher eine konsequente defensive IT-Strategie, die zum Ziel hat Sicherheitslücken zu schließen, die Bevölkerung im IT-Bereich zu qualifizieren und alle digitalen Geräte konsequent zu schützen.

Im gleichen Zug müssen staatliche Allmachtsfantasien von Kryptografie-Verboten, staatliche Backdoors oder Rückangriffe über HackBacks dringend unterbunden werden. Es ist nicht möglich, dass solche Werkzeuge existieren, ohne dass zusätzliche Angriffsvektoren für böswillige Absichten existieren. Diese können damit niemals Teil einer defensiven IT-Sicherheitsstrategie sein.

Abgrenzung zum „Hacken“

Von der Herstellung und dem Einsatz digitaler Waffen ist das bewusste oder unbewusste Auffinden bzw. „erhacken“ von sicherheitsrelevanten Lücken in IT-Systemen abzugrenzen. Verbunden mit einer Meldepflicht für gefundene Sicherheitslücken ist dies ein Dienst im Sinne der Zivilcourage und muss fester Bestandteil einer defenisven IT-Sicherheitsstrategie sein. Dies zieht eine entsprechende Anpassung des „Hacker-Paragraphen“ §202c StGB nach sich.