

Was meinen die Experten?

Die Definition von Cyberwar ist unter den IT- und Sicherheitsexperten genauso umstritten wie die Einschätzung der aktuellen und zukünftigen Bedrohung.

»Whether it be war on land, at sea, or in the air, or now in cyberspace, war always has a political goal and mode (which distinguishes it from crime) and always has an element of violence [...] the effect must be physical damage or destruction. [...] Knowing when cyberwar begins or ends, however, might be more challenging than defining it.«¹

P.W. Singer
US Sicherheitsexperte und Politikwissenschaftler

»Wer über gute Cybertruppen verfügt, kann unentdeckt und im Geheimen die Machtgewichtungen der Welt entscheidend verändern. Er kann seine Gegner gegeneinander aufhetzen, er kann ihre Wirtschaft schwächen, er kann ihr Wissen stehlen und es zum Aufbau seiner eigenen Wirtschaft verwenden, er kann die internationalen Börsen so manipulieren, dass sie ihm nützen und dem er schaden, er kann im Internet die politischen Meinungen weltweit beeinflussen, er wird der Herr über die Infrastrukturen potentieller Gegner sein – und sollte tatsächlich einer dieser Gegner einmal gegen ihn vorrücken wollen, wird er jedes militärische Gerät, das auf Informationstechnik beruht, frühzeitig infiltriert haben und es bereits beherrschen.«²

Sandro Gaycken
Technik- und Sicherheitsforscher FU Berlin

»Ob es Cyberangriffe gegeben hat ist eine Definitionsfrage und daher strittig. Nationalstaatliche Aktivitäten nehmen allerdings definitiv kontinuierlich zu, das ist leider kein Marketing, so sehr ich mir das auch wünschen würde.«³

Felix Lindner
Hacker und IT-Security-Experte

»Unter Cyberkrieg im eigentlichen Sinn versteht man militärische Operationen, die sich informationstechnischer Systeme und Netzwerke bedienen, um den Feind anzugreifen. Dabei muss der Cyberkrieg von anderen Angriffen auf die Cybersicherheit wie Cyberkriminalität, Cyberterrorismus und Cyberspionage unterschieden werden. Letztere erfolgen vorwiegend durch Teile der Zivilgesellschaft (Einzelpersonen, Gruppierungen oder Unternehmen) und unterliegen der nationalen Rechtsprechung, was mitunter problematisch ist. Im Gegensatz dazu stehen sich im Cyberkrieg ausschließlich öffentliche Akteure gegenüber, deren Beziehungen durch das Völkerrecht geregelt werden.«⁴

François Delerue
Europäisches Hochschulinstitut in Florenz

»For me the definition of war is destruction or damage, not just turning out the lights, but destroying the generator, so it cannot come back on.«⁵

Richard A. Clarke
US-Sicherheitsexperte

»We in US tend to think of war and peace as an on-off toggle. [...] The reality is different. We are now in a constant state of conflict among nations that rarely gets to open warfare [...] What we have to get used to is that even countries like China, with which we are certainly not at war, are in intensive cyberconflict with us.«⁶

Joel Brenner
former Head of US Counterintelligence

»Der Cyber-Hype lässt allerdings stets drei grundlegende Wahrheiten außer Acht: Einen Cyberkrieg gab es weder in der Vergangenheit noch gibt es ihn heute, und es ist auch unwahrscheinlich, dass er künftig ausbricht. Und so hat die Cyber-Ära bisher auch kein neues Zeitalter gewaltsamer Konflikte eingeläutet, sondern ist praktisch vom genau entgegengesetzten Trend gekennzeichnet – dem computergesteuerten Angriff auf politische Gewalt. Cyberattacken verstärken politische Gewalt nicht, sondern verringern sie eher – denn sie erleichtern Staaten, Gruppierungen und Personen zwei Arten von Aggression, die nicht in Kriege eskalieren: Sabotage und Spionage. [...] Was gilt als Krieg? Nach wie vor gibt Carl von Clausewitz, preußischer Militärtheoretiker des 19. Jahrhunderts, die treffendste Antwort auf diese Frage. Er identifizierte drei Hauptkriterien, die eine Aggressions- oder Verteidigungsoperation erfüllen muss, damit sie als kriegerischer Akt definiert werden kann: Erstens sind alle kriegerischen Handlungen von Gewalt oder potenzieller Gewalt gekennzeichnet. Zweitens sind kriegerische Handlungen Mittel zum Zweck: Physische Gewalt oder die Androhung von Gewalt sind Mittel, mit denen sich der Angreifer den Feind gefügig machen will. Und drittens muss ein Angriff im Sinne einer kriegerischen Handlung politische Ziele oder Zwecke verfolgen. Aus diesem Grund müssen kriegerische Handlungen während einer Konfrontation einer bestimmten Seite zuzuordnen sein. Bisher aber hat keine Cyberattacke alle drei Kriterien erfüllt, die meisten nicht einmal eines.«⁷

Thomas Rid
Department of War Studies am King's College London
