Nadja Germann
Bereichsleiterin Weiterbildung Energie des VSE
nadja.germann@strom.ch
Responsable Formation continue Énergie de l'AES
nadja.germann@electricite.ch

Hybride Risiken

Nach einem verlorenen Fussballmatch ziehen enttäuschte Fans wütend aus dem Stadion. In der Innenstadt geraten sie mit Klimademonstranten aneinander. Der Streit eskaliert. Die Polizei setzt Wasserwerfer ein. Videos der Polizeiaktion, Twitter-Meldungen der Demonstranten und Bilder von verletzten Fans zirkulieren innert Minuten in den sozialen Medien. Eine weinende Frau hält ihre Unterarme mit Hämatomen vor die Kameras. Die Stadtpräsidentin ist empört! Gleichentags kommt in Genf der elektronische Zahlungsverkehr in den Geschäften wegen einer Cyberattacke während mehrerer Stunden zum Erliegen. Auf einer Messenger-App kursiert das Gerücht eines Anschlags radikalisierter Covid-Massnahmengegner auf ein Unterwerk in Graubünden.

Dieser hybride Mix aus Ereignissen, wahren Nachrichten, bewusst oder unbewusst geteilten Falschinformationen, Verschwörungstheorien, echten und manipulierten Bildern kann eine Verkettung unglücklicher Zufälle sein – muss aber nicht. Er zeigt exemplarisch das Risiko-Potenzial, das in der bewussten oder unbewussten Vermengung von Halbwissen, On-Dits und gezielter Desinformation steckt.

Der bewaffnete Konflikt, der in Europa ausgebrochen ist, beschränkt sich nicht auf die physische Welt. Die «hybride Kriegsführung» bezeichnet eine Kombination aus klassischen Militäreinsätzen, wirtschaftlichem Druck (zum Beispiel durch Rohstoffverknappung), Cyber-Angriffen, terroristischen Anschlägen, Fehlinformationen und Propaganda in Medien und sozialen Netzwerken. Diese Mittel werden offen oder verdeckt eingesetzt, um die öffentliche Meinung zu beeinflussen und Gesellschaften zu destabilisieren. Hybride Angriffstaktiken orientieren sich nicht an Landesgrenzen.

Mitarbeitende und Betreiber von kritischen Infrastrukturen sind in solchen Szenarien als Mitglieder der Gesellschaft und besonders in ihrer beruflichen Funktion gefordert. Um solchen hybriden Gefahren zu begegnen, existieren Konzepte, welche jedes Unternehmen anwenden kann: «Awareness», also das Bewusstsein, dass solche Gefahren existieren, kritisches Hinterfragen von Informationen und Bildern, Abstraktionsvermögen gepaart mit Methoden eines adäquaten Risk-Managements und aktuelle Schutzkonzepte zur Sicherung der IT-/OT-Sicherheit und der Cyber-Security. Der VSE vermittelt Hintergrundwissen und stellt Ihnen Instrumente zur Verfügung, die Sie bei der Wahrnehmung Ihrer Verantwortung, auch im hybriden Bereich, unterstützen.

Risques hybrides

Après une défaite en football, des supporters déçus sortent en colère du stade. Dans le centre-ville, ils en viennent aux mains avec des manifestants pour le climat. La rixe dégénère. La police a recours à des canons à eau. En l'espace de quelques minutes, des vidéos de l'intervention policière, des messages Twitter de manifestants et des images de supporters blessés circulent sur les réseaux sociaux. Une femme en pleurs montre aux caméras les hématomes sur son avant-bras. La mairesse de la ville est outrée ! Le même jour, à Genève, le trafic électronique des paiements dans les magasins est paralysé pendant plusieurs heures à cause d'une cyberattaque. Sur une application de messagerie, une rumeur court : des opposants aux mesures anti-Covid radicalisés auraient attaqué une sous-station dans les Grisons.

Ce mélange hybride d'incidents, d'informations réelles, d'intox partagées consciemment ou inconsciemment, de théories du complot, d'images authentiques et manipulées peut être un enchaînement de hasards malheureux – mais n'en est pas forcément un. Il montre de manière exemplaire le potentiel de risque existant lorsque l'on mixe consciemment ou inconsciemment des connaissances superficielles, des on-dit et de la désinformation ciblée.

Le conflit armé qui a éclaté en Europe ne se limite pas au monde physique. La « guerre hybride » désigne une combinaison d'opérations militaires classiques, de pressions économiques (par exemple à travers la raréfaction de matières premières), de cyberattaques, d'attentats terroristes, de fausses informations et de propagande dans les médias et sur les réseaux sociaux. Ces moyens sont utilisés à la fois ouvertement et de façon masquée dans le but d'influencer l'opinion publique et de déstabiliser les sociétés. Les tactiques d'attaques font fi des frontières nationales.

Dans ce genre de scénarios, le personnel comme les exploitants d'infrastructures critiques sont mis à l'épreuve en tant que membres de la société, mais surtout dans leur fonction professionnelle. Pour affronter ce type de dangers hybrides, il existe des concepts que toute entreprise peut appliquer : l'« awareness », soit le fait d'avoir conscience de l'existence de ces dangers, la remise en question critique d'informations et d'images, la capacité d'abstraction associée à des méthodes de gestion du risque appropriées, et des concepts de protection actualisés pour garantir la sécurité IT/OT et la cybersécurité. L'AES transmet des connaissances de fond et met à votre disposition des instruments qui vous aideront à assumer votre responsabilité, aussi dans le domaine hybride.