Bedrohung aus dem Cyberspace

Bedrohung aus dem Cyberspace

Zu Beginn dieses Jahres trafen sich Fachleute und Interessierte aus Militär, Wirtschaft und Verwaltung zu einem exklusiven, hochkarätig besetzten Event. Das Thema des Anlasses war brandaktuell: Chancen und Risiken der digitalen Welt. Gastreferat und Podiumsdiskussion drehten sich um moderne Cyber-Bedrohungen und unseren Umgang damit.

Bruno Fuhrer

Als Technologie-Konzern, der sich in der Cyber-Security stark engagiert und über viel Erfahrung in diesem Bereich verfügt, war die RUAG prädestinierter Gastgeber. Dabei wurde Wert darauf gelegt, Diskussionsteilnehmer mit unterschiedlichen Hintergründen und Sichtweisen auf die Thematik einzuladen. Entsprechend interessant fiel der Abend für alle Anwesenden aus.

Eine Herausforderung für die RUAG

In seiner Begrüssung verlieh Dr. Markus A. Zoller, CEO von RUAG Defence, seiner Freude darüber Ausdruck, dass

«Die Gefahr von Cyber-Attacken ist auch in der Schweiz real.»

nicht nur die Bühne prominent besetzt war, sondern auch das Publikum. So fanden sich hochrangige Armeevertreter, führende Mitarbeitende von Unternehmen mit kritischer ICT-Infrastruktur und von öffentlichen Stellen sowie diverse Chief Information Officers (CIO's) unter den Teilnehmern – jene Fachleuten also, die sich täglich mit dem Thema Informationssicherheit in ihren Betrieben auseinandersetzen. Nach einer kurzen Vorstellung des RUAG-Konzerns und dessen Leistungen insbesondere im Bereich Cyber-Security kam Zoller auf das Thema des Abends zu sprechen. Die Digitalisierung der Kampfzone stellt für ein Unternehmen in der Sicherheits- und Verteidigungsindustrie eine besondere Herausforderung dar. Schliesslich will man den modernen Bedrohungen aus dem Cyberspace etwas Wirksames entgegensetzen. Zoller zeigte auf, dass die RUAG bereit ist, die Herausforderung anzunehmen, und dass sie in der Entwicklung und Herstellung von Technologie zum Schutz gegen Cyberattacken militärischer und ziviler Art eine Vorreiterrolle einnimmt.

Die Bedrohung ist real

Anschliessend wurde der Gastreferent vorgestellt: William Hagestad II, international anerkannter Fachmann auf dem Gebiet der Nutzung von Computersystemen und Informationsnetzwerken als strategische Waffen. Hagestad ist ein weltweit gefragter Referent zu den Cyber-Aktivitäten Chinas im Informationszeitalter und er hat dazu diverse Bücher publiziert. Das Referat des Cyber-Spezialisten durfte mit Spannung erwartet werden. Lt Col Hagestad, der nicht nur fliessend Mandarin-Chinesisch spricht, sondern auch einen Master of Science in Militärstrategie hält und Sicherheitstechnologie und Technologiemanagement an der University of Minnesota studiert hat, präsentierte erstaunliche Fakten und Analysen zu den aktuellen Cyberbedrohungen, denen sich internationale Verteidigungs- und Sicherheitsorganisationen, aber auch Grosskonzerne und Unternehmen aus der Pri-

«China ist im Bereich Cyber-Spionage besonders aktiv.»

vatwirtschaft heute ausgesetzt sehen. Mit konkreten Beispielen aus der Schweiz und Deutschland machte er deutlich, dass die Gefahr nicht nur die USA oder andere bedeutende Militär- und Wirtschaftsmächte bedroht, sondern auch bei uns real ist.

Angriffe von verschiedenen Seiten

Die Akteure im Bereich Cyberkriminalität und deren Absichten sind äusserst vielseitig. Es sind dies zum einen staatliche Behörden, die in erster Linie militärische und politische Ziele verfolgen und sich mit Cyberspionage Informationen beschaffen. Dann gibt es kriminelle Organisationen, die sich mit Cyberangriffen – und damit einhergehenden Erpressungen

«Podium und Zuschauerreihen waren hochkarätig besetzt.»

von Unternehmen und Organisationen, wie dies etwa der Genfer Kantonalbank erst vor wenigen Wochen passiert ist – finanziell bereichern wollen. Und nicht zuletzt stellt der internationale Cyberterror eine echte Bedrohung für Sicherheit, Ordnung und Frieden weltweit dar, insbesondere weil dieser dezentral operiert und dadurch schwer zu lokalisieren und zu bekämpfen ist. Hagestad betonte aber auch, dass man sich gegen Cyberangriffe durchaus verteidigen kann, wenn man sich der Gefahren bewusst ist, wenn die Beauftragten für Informationssicherheit in Behörden und Unternehmen entsprechend ausgebildet sind und wenn man mit den sich verändernden Bedrohungen à jour bleibt. Letztlich sei das natürlich immer auch eine Kostenfrage.

China als staatlicher Cyberaktivist

Im zweiten Teil seines Referats kam Hagestad auf China als besonders aktiven Teilnehmer im Cyberspace zu sprechen. Die Tatsache, dass China – unter anderem mit einer militärischen Spezialein-

heit – im grossen Stil auf Cyberangriffe zur Informationsbeschaffung setzt, stellt eine besorgniserregende wirtschaftliche und militärische Bedrohung für den Rest der Welt dar. Dabei verwies er auf seine drei bisher publizierten Bücher über Chinas Einsatz von Computernetzwerken als

«Die Angreifer verfügen stets über die neueste Technologie.»

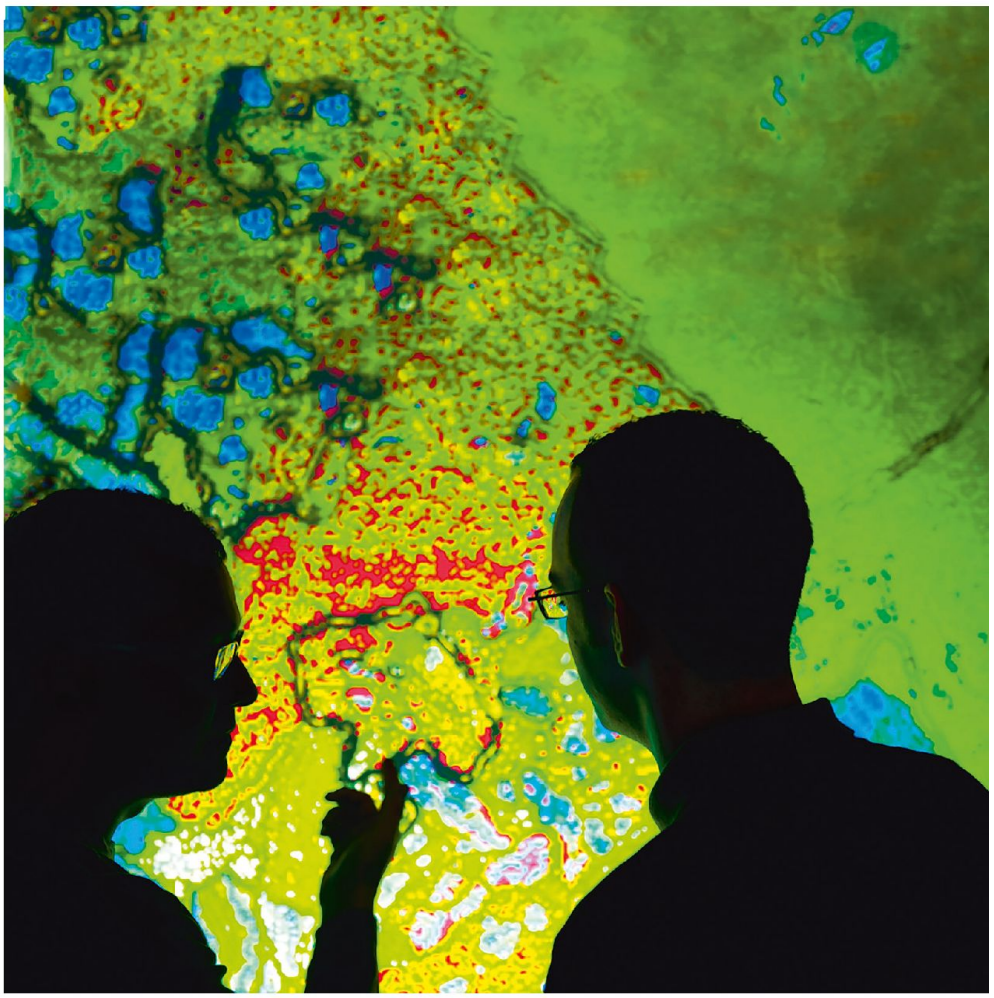
strategische Waffen in einem eigentlichen Cyberkrieg. In diesen legt der Strategieexperte die Ergebnisse seiner jahrelangen Recherchen und Analysen dar und zeigt die Entwicklung seit Mitte der 1990er-Jahren bis in die Gegenwart auf, aber auch die Ziele, die die Cyberangreifer heute und in Zukunft verfolgen. Gerade diese Ausführungen machten deutlich, wie wichtig die laufende Forschung und Entwicklung auf dem Gebiet der Cyber-Security auch bei uns in der Schweiz ist, da in dieser asymmetrischen Bedrohungssituation die Angreifer stets mit neuester Technologie aufwarten. Er appellierte an die militärischen, politischen und wirtschaftlichen Führer, dass eine Zusammenarbeit und ein steter Austausch notwendig sei, um das Bewusstsein für die Gefahr zu fördern und um wirksame technologische und juristische Massnahmen ergreifen zu können.

Geballtes Expertenwissen auf dem Podium

Gesprächsstoff für die anschliessende Podiumsdiskussion war also genügend vorhanden. Unter der Leitung von Zoller diskutierten Gastreferent Hagestad und eine hochkarätige Runde unterschiedlicher Gäste: Divisionär Hans-Peter Walser, Chef Armeestab, ist an der Schnittstelle der politisch-strategischen und operativ-taktischen Bereiche ganz direkt mit dem Thema Informationssicherheit konfrontiert. Zukunftsforscher Dr. Andreas M. Walker gehört in seinem Fachgebiet zu den führenden Köpfen im Land und berät Mandanten aus Politik, Verwaltung und Wirtschaft zu Chancen und Risiken der Zukunft und zum Umgang mit vorhersehbaren und nicht-vorhersehbaren Entwicklungen. Komplettiert wurde die Runde durch Andreas Wuchner, den CTO Security Innovation von HP Enterprise Security Services, der als hoch qualifizierter Fachmann für IT- und Informationssicherheit im Gespräch aus zwanzig Jahren Erfahrung auf seinem Gebiet schöpfen konnte. Die Zusammensetzung der Podiumsrunde sorgte für eine vielseitige, engagiert geführte Debatte, die einmal mehr die Komplexität des Themas

«RUAG ist führend auf dem Gebiet der Cyber-Security.»

deutlich machte. So wurde über die Folgen der Cyberbedrohung für Militär, aber auch für die Zivilgesellschaft diskutiert, über die konkrete Bedrohung der Schweiz und die verschiedenen Möglichkeiten, damit umzugehen. Zum Schluss kam die Frage auf, ob es ein gemeinsames Verständnis über die tatsächliche Situation und die zu treffenden Massnahmen in einer so umfassenden Thematik wie der Cybersicherheit überhaupt geben kann, angesichts der divergierenden Interessen,



«Visualisiertes Netzwerk, überwacht von Cyber-Spezialisten». Bild: RUAG

die in Militär, Wirtschaft, Verwaltung und Gesellschaft bestehen. Eine abschliessende Antwort auf diese spannende Frage liess sich freilich nicht finden.

Positives Fazit

Die RUAG zog als Veranstalter ein positives Fazit und sah sich darin bestätigt, dass ihr aktive, führende Rolle in der Schweizer Cyber-Community durchaus gefragt und berechtigt ist. Es kann mit Gewissheit gesagt werden, dass der Event der Aktualität und der Brisanz des Themas gerecht wurde, und dass sämtliche Teilnehmer neue, wichtige Erkenntnisse in ihr Arbeitsumfeld mitnehmen konnten. ■

Oberstlt a D
Bruno Fuhrer
RUAG
4588 Unterramsern