International Cybersecurity Congress

(Moscow, 5-6 July 2018)

Am 5. Juli Besichtigung des Speicherzentrums für elektronische Daten der Sberbank. Im Security Operation Center wird die Abwehr eines simulierten Angriffs auf den Sberbank Datenspeicher vorgeführt. Das Szenario war ein Angriff mit dem Virus „ Schifrowtschiki“ nach der Methode eines „Distributed Denial of Service“. Dem Security Operation Center ist es gelungen das Problem zu eruieren, zu lokalisieren, Teile des Computernetzes abzuschalten sowie dessen Funktion in der Folge wieder herzustellen (Desinfizierung).

An den Aktivitäten des ersten Konferenztages nahmen ausländische und russische Gäste Teil. Einige von ihnen könnten für die geplante DER-Digitalisierungskonferenz im November d.J. eingeladen werden :

- **Ambassador Andrey V. Krutskikh**, Special Representative of the Russian President for Cybersecurity
- **Dmitriy G. Gribkov,** Security Council of the RF
- **Prof. Anatoly A. Streltsov**, Vice-Director of the institute for Information Security, Moscow State University
- **Stanislav K. Kuznetsov**, Deputy Chairman of Sberbank

(Siehe beiliegende Kopien ihrer Visitenkarten)

Am 6. Juli fand im Moskauer World Trade Center der erste **International Cybersecurity Congress (ICC)** statt. Die Veranstaltung mit hunderten Teilnehmern **wurde von Herman Gref eröffnet**. Dieser erklärte eingangs, dass sich heute weltweit ein Großteil der Wirtschaft auf dem Weg zur Digitalisierung befinde. Parallel zu dieser Entwicklung nehmen die Angriffe im Internet überproportional zu. Der durch Cyberangriffe weltweit entstandene Schaden hat 2017 bereits US$ 1.000 Mrd betragen (Erpressungsgelder). Die größte Gefahr besteht dabei für den Finanzsektor. Gefährdet sind aber die gesamte Wirtschaft und die persönliche Freiheit der Internet User. Die Errichtung von „Schutzmauern“ im Internet sei keine Lösung, da dies Wirtschaft schwer beeinträchtigen würde.

First Session: *Transparant digital world – A trap or a blessing?*

Nick Bostrom (Director / Future of Humanity Institute): Das Internet kann politische Systeme und unsere ganze Zivilisation verändern.

Marc van Zadelhoff (General Manager, IBM Security): 55% der Sicherheitsprobleme sind die Folge von Fehlern der Internetuser. Es mangelt an Verständnis für die Gefahren im Netz. Wir befinden uns in einem Kampf zwischen „Gut und Böse“ mit Hilfe künstlicher Intelligenz. AI wird von Angreifern und Verteidigern eingesetzt.

Penny Lane (Vice President, Payment Fraud Disruption, Visa inc.): Wichtig ist eine regelmäßige Überprüfung der Sicherheitssysteme der Unternehmen.

Yevgeny Kaspersky (Kaspersky Laboratries):“ Meine Firma stört nicht nur Kriminelle sondern auch Staaten“ (!). Mauern können im Internet nicht trennen, sie sind immer durchlässig. Industrielle Revolution 4.0: Eine voll digitalisierte Wirtschaft ist viel schneller als die heutige; Unternehmen, die nicht mitmachen verlieren. Anstelle von Sicherheit wird Immunität der elektronischen Netze benötigt. Ein Einbruch im Netz muss teurer sein als dessen Verteidigung.

Second Session: *Do we have a chance to make the transitional world safer?*

Maxim Akimov (Deputy Prime Minister of the RF**):**
Es geht nicht nur um die Sicherheit Russlands sondern um globale Sicherheit. Wichtig ist der Beitrag jedes Einzelnen zur Sicherheit des Netzes. Den Kampf gegen Cyberkriminalität muss der Staat im Einvernehmen mit der Wirtschaft führen.

Herman Gref: Zusammenarbeit von Staat und Wirtschaft ist entscheidend für Sieg über Cyberkriminalität. 96% der weltweiten Cyberangriffe können abgewehrt werden, 4% aber nicht. 80% der Hacker sind jünger als 20 Jahre; Hacking ist für sie ein Spiel.

Troels Oerting Jorgensen (Head of the Center for Cybersecurity, World Economic Forum): Die Kriminalitätsrate im Netzist zu hoch, sie muss zumindest reduziert werden. Trotz politischen Misstrauens müssen EU, RF, US und China zur Kooperation bewogen werden. Wir benötigen gemeinsame Strategien, Politiken und Standards im Kampf gegen Cybergefahren. Auf globaler Ebene sollte eine 24 Stunden operierende Task Force eingesetzt werden. „Trust is a major competitive factor in business; people will move out of businesses with low security.“
Sberbank war der Initiator des WEF – Security Center.

Meng Hongwei (President INTERPOL): Cybercriminals sind den Cyberdefenders zu meist um einige Schritte voraus.

Margarita Simonyan (Editor-in-Chief, Russia Today): Angriffe mit Cybertechnologie können ebenso großen Schaden anrichten wie mit Atomwaffen (!)

Putins Auftritt beim ICC

Digitalisierung ist Teil der modernen Entwicklung eines jeden Staates, jeder Wirtschaft. Dabei ist die freie Nutzung des Netzes entscheidend, aber auch eine verantwortungsbewusste Nutzung und die Kenntnis der damit verbundenen Risiken.

Die Entwicklung der Cybertechnologie erfolgt in Russland in enger Zusammenarbeit von Staat und Wirtschaft. Wir brauchen Sicherheit im globalen Informationsraum. Die Angriffe auf Russland haben heuer um ein Drittel zugenommen. Wir müssen offen sein und wollen hoffen, dass die Anderen auf unsere Offenheit positiv reagieren.

Medienberichte über Putins ICC Statement sind beigeschlossen.

Während einer Konferenzpause stellte der Sonderberater Putins für Cybersecurity (Krutskikh) die rhetorische Frage: Wie soll es Vertrauen und Sicherheit im Netz geben, solange Cyberangriffe auch Teil einer hybriden Kriegsführung sind?