Beat: Business

CHINA & US HOST MUNICH SECURITY CONFERENCE

CAN WE DISRUPT CYBER-DISRUPTION?

Stanford, CA, 17.11.2016, 16:26 Time

USPA NEWS -

The protection of US critical infrastructures and safeguard of digital growth took center stage at the Munich Security Conference first time held at Stanford University. China´s role as a global player is now the focus of the Beijing conference.

During the first week of November, at the invitation of the Chinese government, the Munich Security Conference (MSC) hosted a Core Group Meeting in Beijing. Topics of the Core Group Meeting, which is co-organized by the Chinese People's Institute of Foreign Affairs (CPIFA), included regional security in the South Pacific, China´s role in the global security order, and the geopolitical implications of the "New Silk Road". In the US, the conference which was co-sponsored by Deutsche Telekom ,was hosted by the Center for International Security and Cooperation at the Freeman Spogli Institute for International Studies at Stanford University September 19 & 20.

As the number of connected devices grows, so does the potential threat for a massive IoT breach. Connectivity has its perks, but it also has risks. Automated data sharing on an "Internet of Everything" scale is an invitation to hackers, especially when security isn´t built into every connected device. The Internet of Everything is here. By 2020 there will be 21 billion connected devices in the market; 5,5 million new devices are added daily.

With physical safety being open and at risk, there is no room to be lax in securing data and IoT devices. Technological changes will store biometrics like fingerprints, personal information, family relationships, secret liaisons, hospital records and much more. Stakeholders from different industries and backgrounds have to cooperate address and ultimately solve the privacy and security problems facing IoT. Educated experts in cyber- economics are needed to safeguard digital growth and establish binding, international cyber-norms agreements. According to Latha Reddy, a member of the Global Commission on Internet Governance and former Deputy National Security Advisor of India, governments could provide leadership in the development of norms and rules, but in the end, a multi-stakeholder approach would be crucial.

In a similar vein, the value of the cyber security market still amounted to only about a fifth of the known damages, with a high number of unreported damages on top. "Most people have no idea that they have been the victim of a cyber crime or data breach, the risk of punishment is extremely slim, the chances of ending up in a courtroom after committing a cyber crime is one in a million or higher" said Marc Goodman, the Chair for Policy, Law and Ethics at Singularity University.

Potentially deadly vulnerabilities are found in billions of devices banks, governments, insurance companies to small businesses. Speaking from the perspective of a service provider, Deutsche Telekom's Senior Vice President Thomas Tschersich noted that companies had to fight thousands of attackers at the same time while the attackers had to be successful only once: "This is not a level playing field." Tschersich and others also stressed the importance of usability and product design that made it easy for customers to protect their data.

Panel members were particularly concerned with the structure of the US election system made and its vulnerability to foreign attacks. Under Chatham House Rule, Russian involvement, disruption at DNC and information leaks during US elections. "This operation follows a script that had been tried before in Ukraine". One participant emphasized that Russia or other foreign agents could not "steal" the election, but that they were able to raise significant doubts about its legitimacy. The inevitable happened of course.

While discussing the quest for international cyberspace norms, terrorist and criminal uses of the internet, Microsoft´s

Scott Charney pointed out that more industry representatives should be included, moving from discussion only to implementation. Gundbert Scherf, the Commissioner for Strategic Management of Armament Activities in the German Ministry of Defense, underlined that cyber was becoming ever more important for the German armed forces and argued that different ministries and sectors had to work together: "Governmental silos won't work when battling cyber vulnerabilities." Deutsche Telekom´s Thomas Kremer had also underscored the importance of collaboration in fighting cyber-crime: "Our chances to fight cyber crime are far greater when we collaborate", stressing "Our responses to cyber threats have to become smarter“.

As for now: In Cybersecurity We Trust. Not.

Article online:
https://www.uspa24.com/bericht-10016/china-und-us-host-munich-security-conference.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Ina von Ber

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report. Ina von Ber

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619