ATILA Lectures

evword(a

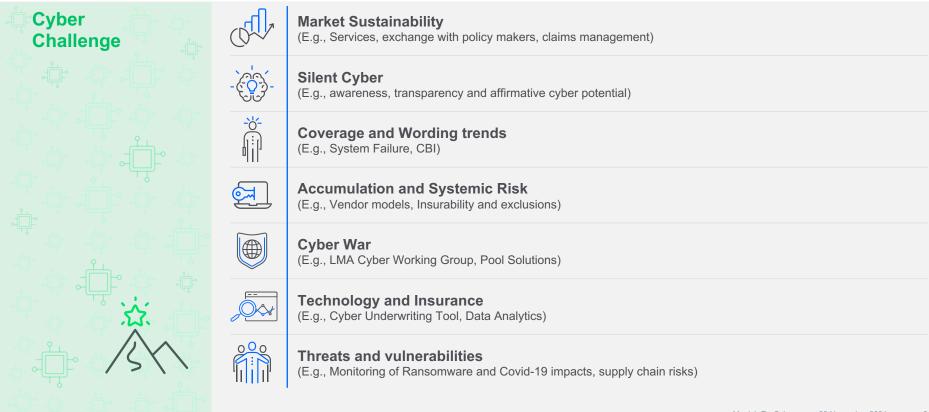
Challenges of (Non-) Insurability of Cyber War and Cyber Terrorism in Cyber (Re-) Insurance

11th November 2021 Franz Gromotka



Current "hot" topics we are actively addressing





Munich RE 🗐

Cyber "War" ? 2017 with a wakeup call



The NotPetya cyber attack that was originally targeted at Ukrainian companies during the Crimean conflict between Russia and the Ukraine. The malware rapidly affected numerous companies, private and governmental organizations, creating significant economic and insured losses across all geographies. In the wind-up, standalone cyber policies as well as policies in "traditional" LoB's ("**Silent Cyber**") came into focus.

Image: mauritius images / DWD-Comp / Alamy

Traditional war exclusions

Existing challenges



consequence of war "the kinetic debate" acts of foreign enemies, hostilities "the grey area / the attribution debate"

"directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order of any government or public or local authority; except that this exclusion shall not apply to cyber terrorism"

declared "declared war is rare" not apply to **cyber terrorism** "can we drive a truck through this <u>carveback</u>?" Cyber Risk

Source: NetDilligence Cyber War & Terrorism Webinar; March 22-25, 2021

Traditional war exclusions

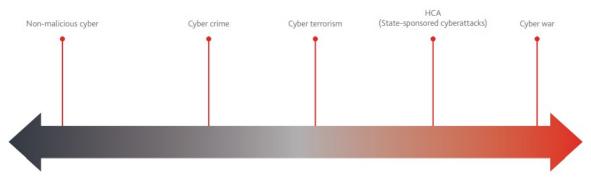
Existing challenges



 No standard or industry alignment so far ("whether declared or not", "warlike operations", "kinetic war")

> Ambiguous with respect to what is considered war in the Cyber context and what shall be considered State-sponsored (Attribution is challenging)

Carveback for "*Cyber Terrorism*" – a means to write back everything?



Cyber war exclusions

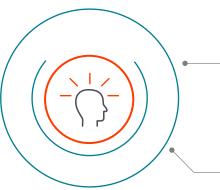
Clarity is key for insured and insurer. Insured must know at every stage what is covered and what not. Insurer wants to offer risk adequate coverage without threatening the balance sheet

> Find solutions on critical aspects such as attribution or collateral damage in dialogue with all stakeholders (Clients, NGOs, Regulatory and Governmental bodies)

Actively consider state involvement and alternative markets for events that go beyond insurability

Munich Re is committed to remaining actively engaged with various stakeholders. As the leading reinsurer in cyber, this is not to promote one standard approach, but rather to have a voice to what may become a widely adopted solution for the pressing challenge of Cyber War

Conclusions





Thank you very much for your attention!

yword(a

Franz Gromotka fgromotka@munichre.com +49 (89) 3891 6360

ndex0f



© 2019 Munich Reinsurance Company