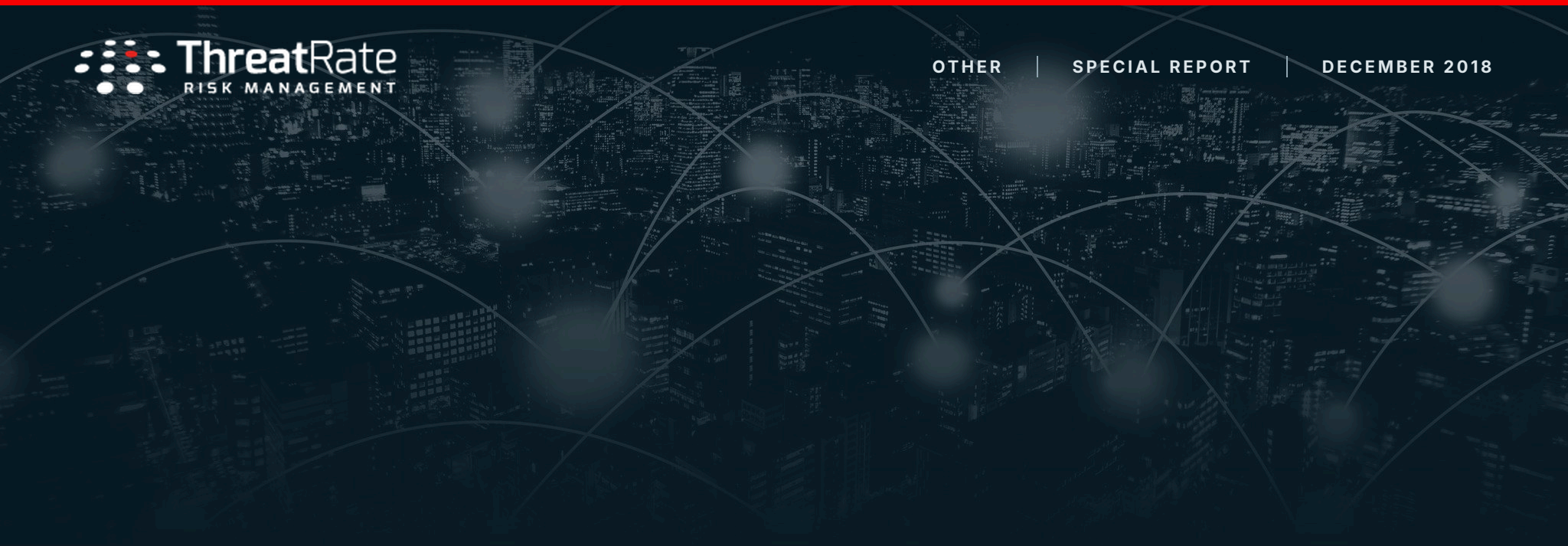


MACRON'S CYBERSECURITY PACT

PUBLISHED
3 December 2018

CATEGORY
Other

OTHER · DECEMBER 2018

Macron's Cybersecurity Pact

Cybersecurity – to most who follow the news or are in any sensitive industry – is acknowledged as a significant issue for private organizations, individuals, and states. There are significant concerns about state actors working with affiliated hacking or cyberespionage organizations to either attack other nations, the critical infrastructure of other states – numerous states in the former Warsaw Pact and Soviet Union have experienced attacks against infrastructure in recent years – or to act on behalf of local companies – sometimes state-owned – and engage in corporate espionage to steal intellectual property (IP) or other research and development materials. On the public side, nations seek to keep confidential material as such and to protect the integrity of public institutions; many democratic societies – notably the United States – are extremely concerned about the integrity of democratic processes as allegations surface against other countries engaging in social media activity to sow dissention; moreover, concerns exist about the integrity of elections themselves as cybersecurity research efforts detail the credible security gaps in election infrastructure.

Seeking to establish ground rules for cyberspace, French President Emmanuel Macron released an international agreement on cybersecurity principles ("Paris Call for Trust and Security in Cyberspace"). The pact was signed by more than one-hundred companies, ninety charities and universities, and more than fifty countries. The ultimate goal of the agreement is to establish what is essentially a digital analogue to the Geneva Convention governing warfare; to further that effect, the agreement proposed numerous measures:

- Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure;
- Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet;
- Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;
- Prevent Information and Communication Technology (ICT) enabled theft of intellectual property, including trade secrets or other confidential information, with the intent of providing competitive advantages to companies or sector;
- Develop ways to prevent the proliferation of malicious ICT and practices intended to cause harm;
- Support efforts to strengthen an advanced cyber hygiene for all actors;
- Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors;
- Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

Despite significant buy-in by many countries, there were some notable countries that declined to sign-on to the agreement. For

© 2018 ThreatRate Risk Management. All Rights Reserved

example, democratic nations such as the United States, Australia, and Israel; relatively unfree or oppressive regimes such as China, North Korea, Russia, Iran, and Saudi Arabia. Many of the countries listed declined to engage with the agreement because of their well-developed and – in cases – extremely active cyberwarfare campaigns. Outside of a well-developed cyberwarfare infrastructure – the United States and Israel's joint efforts on deploying Stuxnet against the Iranian regime is likely going to continue to be known as one of the first significant attacks of cyberwarfare – the United States has other interests that make signing onto this agreement – or similar agreements – highly unlikely. The country's extremely powerful and economically significant Information Technology sector would likely – despite some of companies (notably Microsoft) signing onto the agreement – be the target of many of the regulations that would likely evolve out of an agreement such as the one proposed by Emmanuel Macron. Additionally, given the current administration's skepticism of multilateral agreements – notice the withdrawal from the Paris Climate Accord and the Trans Pacific Partnership (TPP).

While there does seem to be – amongst some countries at least – a general understanding that cyberspace as an evolving front for war – will likely need to have some sort of general rules for conduct to prevent the likelihood of extremely disruptive events from both occurring and leading to escalations – both online and offline.

LIST OF SIGNATORIES OF THE PARIS CALL

- Albanie
- Allemagne
- Autriche
- Belgique
- Bosnie-Herzégovine
- Bulgarie
- Canada
- Chili
- Chypre
- Colombie
- Corée du Sud
- Croatie
- Danemark
- Emirats arabes unis
- Espagne
- Estonie
- Finlande
- France
- Gabon
- Grèce
- Hongrie
- Irlande
- Roumanie
- Royaume-Uni de Grande-Bretagne et d'Irlande du Nord
- Sénégal
- Slovaquie
- Islande
- Italie
- Japon
- Lettonie
- Liban
- Lituanie
- Luxembourg
- Malte
- Maroc
- Mexique
- Monténégro
- Norvège
- Nouvelle-Zélande
- Ouzbékistan
- Panama
- Pays-Bas
- Pologne
- Portugal
- Qatar
- République d'Arménie
- République du Congo
- République tchèque
- Slovénie
- Suède
- Suisse

https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Soundbite analytics

- The United States indicted 13 Russians for election interference.
- Redundant, manual processes allowed Ukraine to recover relatively quickly from a 2015 attack on their electrical grid.
- Nearly 20 years ago, the legal scholar Lawrence Greenberg predicted that international ambiguity around cyberspace would lead to a situation where the United States would be both a belligerent and a victim of cyberwarfare.
- By 2020, there will be an estimated 200 billion connected devices.

© 2018 ThreatRate Risk Management. All Rights Reserved

- From 2017-2021, it is expected that global cybersecurity expenses will exceed one trillion dollars.

SOURCES

1 https://thenextweb.com/security/2018/11/13/heres-why-it-is-unsurprising-that-china-the-us-and-russia-didnt-sign-the-global-cyber-security-pact/

2 https://www.axios.com/cybersecurity-paris-call-for-trust-france-21e434df-8a59-48bc-8cde-cd1c1f43dfd0.html

3 https://securitytoday.com/articles/2018/11/14/us-doesnt-sign-frances-cybersecurity-pact.aspx

© 2018 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2018 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT