

Global Supertrends Forum 2020

The Threats of Today and Tomorrow

Admiral Michael Rogers, Former Director of National Security Agency & Former Commander of US Cyber Command

Anxiety has been the watchword of 2020. Between escalating global political tensions, repeated cyber security threats and the seemingly never-ending global pandemic, there has been plenty for the world to worry about this year.

And it's only natural that we are anxious, says Admiral Michael Rogers, a highly decorated cyber security expert and former director of the National Security Agency.

Admiral Rogers, speaking to the Global Supertrends Forum from his home in Philadelphia, says the world is experiencing an accelerating rate of change amid an epic power struggle between the ideology of the western world and a resurgent China seeking to assert its historical status.

This is an edited Q&A from the discussion.

Should societies be more anxious today than in the past?

Anxiety is an outcome of significant change. And if you look at the world today compared to 20 years ago, you've got both a significant amount of change and an increasing rate of change.

Not only is the rate of change increasing, but change is also increasing uncertainty, which is producing anxiety, frustration, and in many places an undercurrent of anger.

Seventy years ago - in the aftermath of the Second World War - you saw the creation of a significant number of new institutions, from the United Nations to the World Health Organization to alliances like NATO. The creation of these structures and processes was designed to create increased stability.

"Nations are decoupling - pulling the world apart into a series of independent entities."

Now, we have some of the very members that created them, like the United States, questioning whether they

are still valuable and relevant. In the United Kingdom with Brexit, you had a majority of people arguing this construct was not benefiting the United Kingdom. It is also manifesting at a nation state level. For the last 20 or 30 years, technology and business has been driving us to a much more integrated world, yet in the last few years, you're seeing challenges, particularly in the political arena.

This is playing out visibly in the relationship between China and both Australia and the United States.

Nations are decoupling - pulling the world apart into a series of independent entities.

That is a fundamentally different approach than we have had, arguably, for the last 70 years.

COVID is accelerating these changes - but they were already there.

Moving to your speciality of cybersecurity, the increasing role of technology is all encompassing. What are implications for businesses, economies and communities?

The last 10 years has taught us that no-one can isolate themselves from cyber threats. If your strategy is to hope they go after someone else, it is a fundamentally flawed premise.

The good news is there is broad recognition - from nation states to companies and individuals - that cyber security is a priority and requires some level of investment focus.

But what is the best course of action?

Ten years ago, the focus was to stop the opponents.

But there's an increasing realisation in the past one to two years that despite your best efforts, your opponent will potentially get into your system.

Resiliency is key - what can I do to make sure that I can keep operating?

Does that put us at odds with privacy and if so, are western democracies disadvantaged in maintaining security by virtue of the freedoms that we take for granted?

We have built our entire societies - whether Australia or the United States - on the fundamental right of the

individual. One of those rights is the idea that privacy is a core tenet of our societies.

So, there are two challenges.

Number one, what does privacy mean? What does anonymity really mean? And how do you achieve it in this world in which literally everything we do creates a digital footprint?

That will never go away. We deal with that as parents and I can remember talking to my children as teenagers about it.

So you need to be thinking about how you communicate, you need to be thinking about what are the implications for this digital footprint that you're creating and what might seem perfectly appropriate when 15 or 16, may not seem like such a good choice when you're in your 20s or 30s.

Two, in counterterrorism efforts do you - in the name of security - adopt practices or policies that arguably are fundamentally against the morality and the values of your society?

If we walk away from our values in the name of security, I would argue the adversary has won.

Is technology our friend or foe?

It is the new normal. We're not going back. We can't erase these footprints. If I engage in this digital world, my only option is to create these footprints.

Some say go the opposite direction - walk away from it. That is not workable. Economies can't function without it.

Think about the quality of life advantage we get from the ability talk to our family, see images of the world around us, access knowledge to a level that literally no other people in the world prior to the last couple decades have ever had access to.

"We have built our entire societies - whether Australia or the United States - on the fundamental right of the individual. One of those rights is the idea that privacy is a core tenet of our societies."

So technology has positive aspects and it has negative aspects.

The challenge is that technology must be applied within a social framework of values and morality. You can't pretend that technology is somehow separate from all that.

That's one of the reasons why you are seeing pushback against technology companies.

We're very comfortable with the use of technology at work and in our day to day life - we embrace

technology and we're grateful for what it's capable of doing - yet we find ourselves saying that the people that created, monetize and run these organizations make me nervous.

So that's an interesting trend to watch out how this is going to play out in the coming years.

Can companies hope to prevent sophisticated state actors accessing data, or is it just a case of limiting the damage?

For criminals, they tend to work on volume and scale. They want to hit as many targets as they can, as quickly as they can and then move on.

For nation states - and I was one - they tend to focus on targets for extended periods of time, and they are willing to invest resources for an extended period of time.

So that can make things harder on the corporate side.

What are the risks of cyber security issue leading to a dislocation on markets?

I would argue that the virtual world has actually proven more resilient than the physical. You look at major storms - we literally spend weeks, months, years in reconstitution.

But you look at cyber events - the effects are largely dealt with within a number of weeks or days.

So I would say history has shown the virtual world is more resilient.

Is COVID-19 opening us up to vulnerability on the cyber security front?

I do believe there is increased cyber security risk from COVID.

Why? Because we went from a very structured, layered defence in companies built around the idea of physical proximity where we were working in offices.

COVID comes along and we have had to push out connectivity to homes. We're blurring the lines between what is home, and what is work, on the same systems, the same backbone. We're all doing work. Our children are doing games and schooling, our spouses and family members are doing business - and we're all using the same backbone. Security becomes much more challenging.

Is Australia striking the right tone with its national security attitude towards China?

I encourage nations to be realistic and be direct.

Let's not pretend these things aren't happening.

Rather, let's ask ourselves how do we educate our public, how do we educate our economy, our businesses and how do we improve our cybersecurity and our cyber resilience?

At the same time, how do we take steps to clearly communicate to other nations: we know what you are doing, we believe that this is unacceptable and we're prepared to engage in a series of steps to get you to stop. It's not because we want to make you an enemy, it's not because we're diametrically opposed. It's because you have chosen to engage in a series of activities that work against the national security of my nation and the economic well-being of my citizens and their privacy.

"We're blurring the lines between what is home, and what is work, on the same systems, the same backbone. Security becomes much more challenging."

What do you think China's goal is?

Broadly, the strategy of the Chinese government is to ensure the control of the Party.

You also have to acknowledge social norms in China are different.

In order to ensure the long-term control of the party the government has to ensure the economic well-being of its citizens.

I also believe that China has watched the last hundred plus years – which they view as an aberration and they call the century of humiliation –they believe the position of China in the world has been out of step with what was the historically normal.

They have come to the conclusion that the rest of the world created the technologies that led to advantage in the post-World War Two era and particularly in the case of America, created these enormous companies that took that technology, monetized it and applied it on a global scale.

As they look forward their view is they want to change that dynamic. And the way they change that dynamic is out compete in the fundamental technologies of the digital age: quantum, artificial intelligence, nanotechnologies, etc.

Is the approach of the West in restricting the activities of some Chinese companies valid?

Here's what's playing out. Under Chinese law, the Chinese government has the authority to compel any Chinese entity - individual or company – to provide whatever data the government wants or execute whatever direction.

That is not true in Australia and it is not true the United States. In both of our nations, there are protections

designed to ensure the government can't unilaterally do that.

The challenge is if you are going to accept technology from an authoritarian state in which the legal framework of that state enables them to direct these companies to do what the government wants, are you comfortable with the idea of embedding Chinese technology in certain aspects of your infrastructure?

I think that's a fair question.

Now, I don't think the answer is China bad, rest of the world good.

Rather, I think it is important to say in some areas, the level of risk to our long-term national security and a long-term economic competitiveness is such that we believe we should not allow or enforce a Chinese based solution. I think that's a fair thing.

"Are you comfortable with the idea of embedding Chinese technology in certain aspects of your infrastructure?"

US tech companies are also facing regulatory scrutiny. What do you think right level of scrutiny is?

I think we're in for a real interesting period about the correct role of government. Is it regulation and control or taxation and financial policies? These companies are global in nature. Most of our tax structures are predicated on a bricks and mortar presence – but many of these global companies don't have that physical presence.

So how do I tax you? I think that is a fair question.

The flip side is, if we're not careful and we take this to the extreme, we'll end up killing the goose that laid the golden egg. These companies have created some amazing technology and have increased quality of life.

I want to make sure that even as we're asking ourselves what is the right level of government oversight that we don't end up destroying that.

Finally, what positive note can we end on? What is something we should feel good about in the West?

Australia and the United States are societies that embrace the idea of innovation, embrace the idea of competition and embrace the idea of the rights of the individual.

When you've got fundamentals that are solid like that, you can do great things.

What we need to do now is build on those.

Let's take advantage of the fact that our societies are willing historically to take on hard problems, we're willing to work hard and not only to support ourselves and our nation, but to try to help the broader world around us.

We can do some great things.

Disclaimer

This material has been prepared by CREDIT SUISSE GROUP AG and/or its affiliates ("Credit Suisse").

It is provided for informational and illustrative purposes only, does not constitute an advertisement, appraisal, investment research, research recommendations, investment recommendations or information recommending or suggesting an investment strategy, and it does not contain financial analysis. Moreover it does not constitute an invitation or an offer to the public or on a private basis to subscribe for or purchase products or services. Benchmarks, to the extent mentioned, are used solely for purposes of comparison. The information contained in this document has been provided as a general commentary only and does not constitute any form of personal recommendation, investment advice, legal, tax, accounting or other advice or recommendation or any other financial service. It does not take into account the investment objectives, financial situation or needs, or knowledge and experience of any persons. The information provided is not intended to constitute any kind of basis on which to make an investment, divestment or retention decision. Credit Suisse recommends that any person potentially interested in the elements described in this document shall seek to obtain relevant information and advice (including but not limited to risks) prior to taking any investment decision. The information contained herein was provided as at the date of writing, and may no longer be up to date on the date on which the reader may receive or access the information. It may change at any time without notice and with no obligation to update. To the extent that this material contains statements about future performance, such statements are forward looking and subject to a number of risks and uncertainties. It should be noted that historical returns, past performance and financial market scenarios are no reliable indicator of future performance. Significant losses are always possible.

This material is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of, or is located in, any jurisdiction where such distribution, publication, availability or use would be contrary to applicable law or regulation, or which would subject Credit Suisse to any registration or licensing requirement within such jurisdiction. The recipient is informed that a possible business connection may exist between a legal entity referenced in the present document and an entity part of Credit Suisse and that it may not be excluded that potential conflict of interests may result from such connection.

This document has been prepared from sources Credit Suisse believes to be reliable but does not guarantee its accuracy or completeness. Data sources, Credit Suisse unless otherwise specified.

Credit Suisse may be providing or have provided within the previous 12 months, significant advice or investment services in relation to any company or issuer mentioned, including collaboration on potential product offerings, which may result in the receipt of fees for such services. This document may provide the addresses of, or contain hyperlinks to, websites. Credit Suisse has not reviewed the linked site and takes no responsibility for the content contained therein. Such address or hyperlink (including addresses or hyperlinks to Credit Suisse's own website material) is provided solely for your convenience and information and the content of the linked site does not in any way form part of this document. Accessing such website or following such link through this document or Credit Suisse's website shall be at your own risk. This document is intended only for the person to whom it is issued by Credit Suisse. It may not be reproduced either in whole, or in part, without Credit Suisse's prior written permission.

Copyright © 2020. CREDIT SUISSE GROUP AG and/or its affiliates. All rights reserved.