Prague Security Studies Institute

Pohořelec 6 | 118 00 Praha 1 | Czech Republic
Tel./fax: +420 233 355 735 | email: pssi@pssi.cz | www.pssi.cz

Economics and Technology: Emerging New Threats

Edward Hunter Christie

Remarks delivered at the PSSI seminar on Economics and Technology: Emerging New Threats, hosted by the American Center in Prague

9 November 2021

We live in a world of Great Power competition.
Long gone are the days of simple, US- and EU-led globalisation, in which we could behave as if power politics didn't exist.

The global strategic picture is probably well known to you all but let me lay it out briefly.

Two major security challenges take up a lot of bandwidth today, notably in the United States but also at NATO, across Europe, and really across the Western world. And I will address both. They are the following:

1/ The Rise of China

2/ and the rise of New Technologies, notably Artificial Intelligence

These two major transformative trends are already affecting everything we do, in the private sector, in public policy generally, and in national security and defence policy.

China's economy, if one measures it at Purchasing Power Parities, is already 15% larger than that of the United States. And we should expect China to overtake America also in terms of current exchange rates, perhaps by 2035.
A world in which neither the United States nor the European Union are the biggest economy, or the biggest market, that is very new. It is radically new. During the Cold War, the Western Alliance faced a formidable enemy in the shape of the Soviet Union. But the Soviet Union never came close to overtaking America economically. At the very highest point and using the same type of conversion I used earlier, it may be that the USSR was two thirds of the US economy in equivalent material terms, and that was in the mid 1960s, and it didn't last. By the end of the Cold War, it was more like one third of the US economy. For reference, today, the Russian economy is about 20% of the US economy at Purchasing Power Parities.

China today is not 20%, or one third, or two thirds of the US level, but as mentioned, 115%. It is already larger. And it is still growing, faster than the United States or Europe.
The world is changing. Now. This decade.

But that shift, large as it is, doesn't mean the old problems are gone. For Europe, Russia and Islamist terrorism are the most direct potential security threats. China and dynamics in the Indo-Pacific come in addition to the other two – they do not replace them.

We do not get to choose between facing up to Russia versus China versus Islamist threats.
We also do not get to choose what relationships these threat actors may have with each other.
Those choices are theirs, not ours.
It is irrelevant whether someone in the West believes that Russia really ought to see sense and fear China and embrace the West. Maybe that would be sensible, but unless and until Russia actually behaves that way, then we cannot responsibly assume that that is the direction of travel.
In fact, the evidence of the last few years rather suggests the opposite – namely a rapprochement between Russia and China.
We may not like it, but it is not in our gift to choose the policies of other Great Powers.
We can only deal with what they do, and manage our own policies responsibly, by ensuring that we have a highly credible deterrence and defence posture, by protecting our vital interests, by remaining united and well-coordinated in our policy choices, and by applying a healthy dose of alertness and self-control in our dealings with foreign powers.

The general power shift I described is happening at the same time as we're experiencing a major wave of new technological change.

And the biggest transformative technology is Artificial Intelligence, particularly in its contemporary form, meaning Machine Learning, which includes Deep Learning.

It is relevant to remember how world history changed in light of the steam engine, or in light of electrification, or in light of the internal combustion engine. And in more recent decades, through computing and the Internet.

All of these examples are what are called General Purpose Technologies. That is a key concept. We're not talking about limited military technologies, or narrow civilian ones, or what I would call "narrow dual-use technologies" such as laser or thermal imaging.

General Purpose Technologies are far broader, they span a far greater range in terms of areas of application. They transform many areas of life and of economic activity – as well as the world of security and defence.

So, AI is a General Purpose Technology. And AI is going around the planet, and every state, every major organisation, private and public, knows it must invest, adapt, adopt, and move forward.

What does that mean for our security? And what is the connection with China, and indeed with other threat actors?

Well, technology diffuses. That is its wonder, and also its challenge. Humanity doesn't get to move forward without spreading the best technologies around the world. But then no area of life is left untouched. Matters of war and peace, of the strategic balance, of military means, of coercive relations between states, and even non-state actors, that all moves along too.

Russia, for example, is working on AI for military applications.
Of course they are.

China is too.

So, what does it mean for us across the Western World?

It means the race is on. The race is on between the West and China in particular, in very visible ways. That's what the conversation is about – transformation, new capabilities, next-generation capabilities, which will leverage AI and other new technologies.

It is important to understand the magnitude of potential future developments.

AI can improve all types of information processing, pattern recognition, prediction, for any type of data – sets of numbers, text, voice, images, video.

It has been a long time coming but now it is here. Machine Learning outperforms humans in terms of accuracy over a significant range of pattern recognition and prediction tasks.

And with appropriate "eyes and ears" on robotic systems, meaning with good sensors, and with communication technologies, we are looking at a world of intelligent connected devices, capable of determining their own courses of action to solve particular objectives.

With the ability to work effectively:
1/ In teams of machines – swarm robotics is a key expression here
2/ In mixed human-machine teams – a key expression here is human-machine teaming
3/ And alone if they become isolated from their teams and unable to communicate

All of that, in both the cyber realm and in the physical realm. With the potential of higher accuracy, and of course faster information processing and faster decision-making cycles.

This can be true for a range of civilian applications, and for military ones too. Whether it's collaborative robotics on the factory floor – or swarms of autonomous drones in a military operation. That is the general direction of travel, with many new achievements in recent years, and with more to come.

States will necessarily invest in this space. The power implications are too great to ignore, especially once one assumes that potential adversaries will do the same. Which they will.

And with rival powers that have substantial resources and levels of ambition, we must ourselves aim at maintaining our technological edge, as much as possible, for as long as possible.

The policy question then becomes: how do states win technology races, or at least stay ahead or not fall back, within such races?

In short, we need to:
1/ get better at what we're doing at home, and
2/ reduce the ability of foreign powers to have access to what we're doing

This splits naturally between two dimensions: Domestic Innovation Systems, and the External Dimension.
For each dimension, I will now list 9 essential areas of work.

Domestic innovation systems	**External dimension**
R&D subsidies	IP protection (as contested)
Tertiary STEM education	Standardization (as contested)
Research universities	Trade openness with non-rivals
Private venture capital	Trade & investment restrictions on rivals
Government venture capital	Export controls
Government procurement	Foreign investment screening
Innovation networks	Counterintelligence
Innovation clusters	Espionage-related sanctions
Domestic industrial capacity	Espionage vulnerability mitigation

I will focus mainly on the External Dimension and develop a few examples:

1/ trade and investment restrictions on rivals

An example here is Executive Order 14032 of 3 June 2021 by the President of the United States – essentially banning US financial investments into Chinese companies involved in either the military-industrial complex of China, or that are developing surveillance technology to facilitate repression or serious human rights abuses.

You may recall that Huawei, among others, was listed. It is relevant to realise that the key companies of China's aerospace and defence sector are there too. This is much broader than just 5G, or surveillance. We're talking about shipbuilding, aerospace, missile technologies – and surveillance too.

The first version of that order was under President Trump, in November 2020. The one we have now, from June 2021, is slightly amended but really very similar. So, it's important to remark that, on the US side, this is a bipartisan issue.

The rationale is simple, and in my view not controversial at all.
Why should our financial resources be invested in companies that are developing military or intelligence or surveillance technologies at the behest of foreign powers that pursue ambitions and methods that are contrary to both our interests and our values?

In the European context, we already pursue that path towards Russia. We have restrictions in place on financial investments in key Russian defence industry companies, ever since the 2014 sanctions were adopted by the European Council.

2/ foreign investment screening

Screening of Foreign Direct Investment, that is, of strategic investments in corporations in our countries, is an area of policy that has developed further in recent years.

In the United States, strengthened legislation came in 2018 – that's the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which modernized and strengthened the key US structure in this case, which is called CFIUS, The Committee on Foreign Investment in the United States.

In the European Union, we have new EU law, namely Regulation 2019/452 of 19 March 2019 "establishing a framework for the screening of foreign direct investments into the Union".
The regulation establishes a framework for the screening of investments from outside the Union:
1/ for Member States to each carry out (the main work happens nationally)
2/ for Member States to cooperate, with each other and with the European Commission

The regulation is a framework, it leaves a lot of leeway to Member States, but conversely this has allowed for the principles expressed in it to be very sensible and to be stated in clear language.

Article 4 of the Regulation in particular:

Member States and the Commission may consider the following areas, among others – I will just list two of them:

- Critical infrastructure
- Critical technologies and dual use items, including artificial intelligence, robotics, semiconductors, cybersecurity, aerospace, defence, energy storage, quantum and nuclear technologies as well as nanotechnologies and biotechnologies

If you wanted an official confirmation of what key technology areas are considered critical, this is as good a list as any. Similar lists emerge from work in the NATO context and in national strategy documents.

And Member States and the Commission may also take into account certain factors, I will just list the first one:

"whether the foreign investor is directly or indirectly controlled by the government, including state bodies or armed forces, of a third country, including through ownership structure or significant funding"

So, this is just common sense.

The recent Czech law on Foreign Investment screening seems very much to follow this common-sense spirit.
From what I've understood, it ensures there is mandatory notification to the government and an ability to block investments if they would result in providing effective control, by the foreign investor, over a domestic entity, and that the latter engages in manufacturing, R&D, or innovation of military equipment, or it engages in critical infrastructure, or in critical information infrastructure or essential information services, or in manufacturing or developing dual-use items.

3/ Measures against foreign state subsidies that distort competition

Another interesting development on the EU side is the proposed regulation "on foreign subsidies distorting the internal market" of 5 May 2021.

Here we're talking about essential abilities to scrutinize and then take redressive actions in case a company on the EU market benefits from foreign state subsidies. Redressive actions could include orders to carry out divestments, for example, and the regulation would allow for the use of fines in case the company does not take appropriate remedial action.

This approach is broader-based and well within the logic of the Single Market, in which state aid by EU member states is strictly regulated. It was high time that this be applied to what is de facto state aid from foreign states.

4/ Protection of Intellectual Property: Trade Secrets

Under both US and EU law, a trade secret is information that is not generally known or discoverable by others, is maintained in secrecy by its owner (meaning a company), and it gives its owner a competitive advantage because it is secret.

Trade Secrets is one of two main approaches for companies to protect innovative ideas – the other main approach is patents, which relies on the opposite approach, namely publishing the information, but giving a legal monopoly to the patent owner to allow the patent owner to gather income from royalty fees.

Trade Secrets is an area that underwent legislative changes, in both the US and the EU, in 2016, and partly for the same reasons. In both the US and EU context, the combination of the rise of digital technologies and of the rise of China were clearly referenced reasons for strengthening legislation.

And in the case of China, we have clear evidence of cases of state-sponsored economic espionage.

In the United States, the Federal Bureau of Investigation has been very outspoken about this problem, and about its place within the broader challenge of the rise of China. To quote the Director of the FBI, Christopher Wray: "The Chinese government is fighting a generational fight to surpass our country in economic and technological leadership."
And Wray goes on to say that the Chinese, quote, "have shown that they're willing to steal their way up the economic ladder at our expense".

So, we already have updated legislation for Trade Secrets, and that is a good thing. That's just one part. There are many non-legislative measures, including programmes, training, and events to raise awareness about information security in the corporate world and in scientific research institutions for example. And this really concerns both cyber means of intrusion and human intrusions.

These four classes of policy instruments are all different, but they have a few things in common in terms of the general strategic challenge they address.

China seeks an advancement of its technological and economic power.

Distorting competition in its external trade and investments, while also aggressively acquiring technologies, whether through licit means or illicit means, and while also using state subsidies – all of these measures are tantamount to using our Western market principles against us, as a slingshot to propel China ahead of us, by making money from us, and getting our best technologies, and using the former to accelerate the latter, and the latter to enhance the former.

And so, once this is understood, the actions of China's State-Owned Enterprises and other Chinese entities with close links to the Chinese Communist Party should be seen in a different light.

We are talking about a single-party dictatorship with major power potential and major power ambitions – in the economic and industrial realm, as well as in the military and foreign policy realm.

This does not mean that all Chinese corporations are that way, let alone all Chinese people. But it is possible to clearly identify key corporations that we should generally not be doing business with.

So, what next?

We need to start documenting in further detail who these key corporations are, their areas of activity, their linkages with key Chinese state or party institutions. Then there is the question of how they are financed and by whom, in China, in Europe, in America, and elsewhere. For instance, is it the case that European or North American capital markets are used to raise funds for these companies? Of

particular interest, of course, are those companies that are engaged in supplying military, security, surveillance, or intelligence products or capabilities to the Chinese state or to the Russian state.

The more we know, the better we can target justified protective measures.

Protective measures, as mentioned, can include prohibitions on financial investments into certain key entities.

Relatedly, governments on both sides of the Atlantic may wish to block Foreign Direct Investments from those same entities, and entities associated with them.

In parallel, and this now addresses the first set of policy tools I mentioned earlier, Western nations need to provide for dynamic and competitive home-grown innovation ecosystems.

The latter require sources of capital investment they can trust – and they need more of it. It is with that intention that the US Department of Defense launched an initiative for Trusted Capital Marketplace. Recent NATO decisions on the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Defence Innovation Fund follow a similar spirit.

Innovating more and better in crucial technologies – in Emerging and Disruptive Technologies – is now a high priority for decision makers on both sides of the Atlantic.

And the challenges related to doing so securely, bearing in mind the challenges posed by foreign powers such as Russia and China, are a major area for ongoing public policy analysis, adjustment, and maturation.

For example, are our Export Control regimes fit for purpose for the age of AI, autonomy and robotics, quantum technologies?

And do we have a proper whole-of-government approach to ensure, for example, that justified warnings from our counter-intelligence services are listened to and understood – and acted upon – across the machinery of each national government among our nations? And with coordination between our nations?

Do our corporate sectors and higher education sectors have the awareness, expertise, and inclination to detect and respond to espionage attempts, whether by cyber intrusions, or human intrusions?
And are our business and finance communities ready to work constructively on justified matters of national security and international security?

These are important considerations to have in mind as policies continue to develop and mature in the direction of better security awareness and better strategic awareness across Western democracies.

Pohořelec 6 | 118 00 Praha 1 | Czech Republic
Tel./fax: +420 233 355 735 | email: pssi@pssi.cz | www.pssi.cz

And the only way to get there is together and with a clear sense of shared responsibility for our future prosperity and for our future security.

Thank you.