DUTCH
TRANSFORMATION
FORUM

Gaming the new security nexus

A collaborative research paper by KPMG and The Clingendael Institute prepared for the Dutch Transformation Forum

November 2019

Foreword

We are on the verge of large and global changes. Technological breakthroughs from the fourth industrial revolution are affecting our daily lives, meanwhile Western society is being rivalled by strong competitor Asia, and especially China. **How do we plan for security and freedom in such disruptive times?** How does Europe avoid being squashed between America First and the Chinese Dream? How do we leverage the innovations from Artificial Intelligence and the Internet of Things without getting bogged down in geopolitics around 5G?

This paper discusses the new security nexus of security, geopolitics and digitalization. As we will show, these topics are heavily intertwined. China's 'New Generation Artificial Intelligence Development Plan' offers an outlook for them to become the global leader in Artificial Intelligence (AI) by 2030, and their 'Made in 2025'-strategy is aimed for China to become the new global manufacturing, cyber, science and technology innovation superpower. **History teaches us that those who set the technical standards will dominate the world**. Add into the mix China's 'Belt and Road Initiative', which encompasses over 1 trillion USD in investments, establishing China's influence on the Eurasian content by investing in all kinds of physical trade infrastructure, such as dry-ports, shipping routes and railways. We can conclude that **China plans to re-establish both a digital and a physical silk road**.

Meanwhile, this hegemonic shift from West to East motivates other countries to join the power game. This is especially apparent in the cyber security domain, where countries such as Russia, Iran, Israel, North Korea and of course America and China are increasingly active. **Nation state and organized crime driven cyber-attacks** are not only aimed at financial gains, but lately more and more on gaining political influence, acquiring intelligence, preparing for hybrid warfare or disrupting enemy infrastructure. **Dutch companies and governments are well prepared to prevent cyberattacks, but they don't dare to face the inevitable truth that they will be hacked. They are ill-prepared to detect and respond to such attacks**.

The latter is particularly worrying in times where our social dependencies on digital infrastructure is rapidly increasing. Consider examples such as AI managing factories based on sensor-data, autonomous cars or connected-cars based on 5G and image recognition, algorithmic profiling of civilians, social-credit systems based on face recognition. These examples will today or tomorrow change our lives drastically. **How do we manage trust and security in these complicated digital infrastructures that – upon disruption – may lead to social disturbance?**

New strategic leadership is necessary to effectively deal with this new security nexus.
We are now standing at the cross-roads of managing it. How can open society remain strong in the face of foes and its own fragility, without sacrificing – and instead leveraging – its openness? We are convinced that hegemonic and technological changes present us with threats and show us our weaknesses, but we are moreover convinced that these changes offer us opportunities to build on our strengths as a Dutch and European society and benefit from the uncertainty these big changes cause. But to secure this future, we must act now and together to understand and plan for security and freedom.

We are looking forward to a stimulating discussion with you at the Dutch Transformation Forum 2019,

Frans Blom,
Chairman BCG The Netherlands

Tjeerd Bosklopper,
CEO Nationale-Nederlanden a.i., CTO NN Group, Member of the Management Board NN Group

Stephanie Hottenhuis,
Chair Board of Management KPMG Netherlands

Derk Lemstra,
Managing Partner Stibbe

Rob Miesen,
Managing Partner Spencer Stuart

Steven van Rijswijk,
Chief Risk Officer, Member Executive Board ING Group, Member Management Board Banking ING Bank

Monika Sie Dhian Ho,
General Director Netherlands Institute of International Relations Clingendael
(rotating research paper partner DTF)

Peter Zijlema,
CEO IBM Benelux, Country General Manager IBM Netherlands

Introduction

No matter where one lives in the world, or what one's political views, it is clear that we are living in an age of profound change. New technologies, climate change and major shifts of geopolitical and economic power are not part of the future; they are part of the realities of the 21st century. Historians are used to looking backwards in time. Doing so at a time of transformation is particularly important: predicting what lies ahead is difficult. So it is all the more important to spend some time reflecting on how and why we have got to where we are in the world today.

Thirty years ago, in November 1989, the Berlin Wall came down. The years that followed saw the end of Apartheid in South Africa, and major reforms in China. These changes seemed to herald a new age of freedom, of liberty, of democracy.

And here we are, three decades on, confronted by a world that suddenly seems unfamiliar, strange and threatening. The symbolism of walls being torn down has been replaced by the prospect of barriers being erected. In the place of co-operation, collaboration and hope have come competition, rivalry and fear.

It is tempting to think that the roots of these shifts are recent – to assume that the transformation has been sparked by one-off, exceptional factors. But the context is not recent for Brexit, for Donald Trump, for the surge of populism that has given leaders the opportunity to use angry rhetoric to exploit division and consolidate their powers. In fact, all these phenomena are part of a bigger picture, of more fundamental change.

And this is why it so vital to look to history for inspiration and for guidance. Studying the past can help always provide parallels that are instructive. At times of change, identifying what those are is especially rewarding. But above all what history does is to provide context and perspective. The world will keep turning on its axis, as it has always done. What really matters is being able to adapt to new circumstances and to new challenges: being in the right place at the right time brings rewards; getting things wrong can be disastrous.

The first thing to do then is to make sure one is asking the right questions. And there is no better place to do that than in a forum that brings together top leaders from the public and private sector to discuss how best to answer them.

I am greatly looking forward to participating in the Dutch Transformation Forum 2019 – and to following closely the discussions and conclusions that come about as a result.

Peter Frankopan,
Professor of Global History, University of Oxford
Senior Research Fellow, Worcester College
Director of the Oxford Centre for Byzantine Research

Chapter 1
Why we must plan for security and freedom

When the famed philosopher Karl Popper wrote perhaps the most rigorous defence of the **open society** ever written – The Open Society and its Enemies – its fate was all but certain.

It was the 1940s. The young academic had fled his home country of Austria in fear of Nazi persecution. He witnessed the free world fall victim to totalitarianism – and with it the idea that societies based on freedom of information and inquiry will in the end be the most stable and secure.

The big question then was:

How can the open society remain strong in the face of foes and its own fragility, without sacrificing its openness?

Today, Popper's big question is still relevant. The context of the question, however, has changed dramatically, in two ways.

First of all, the geopolitical context is radically different. For the first time since the fall of the Berlin Wall, Western society is faced with a successful rival model: China. As the European Commission said in its recently published **China** strategy: *"China is, simultaneously, […] a cooperation partner […], a negotiating partner […], an economic competitor in the pursuit of technological leadership, and a systemic rival promoting alternative models of governance."*[1] Moreover, the US has shifted its geopolitical course dramatically. President Donald Trump has already said he does not intend to pick up Europe's security bill for much longer. Between America First and the Chinese Dream, Europe seems to be stuck in the middle.

Second, it is a fact that the digital revolution brings us profound changes. It has been transforming information flows, it disrupts the global economy – and indeed the social cohesion of our societies – in ways that fundamentally challenge the way we think about the **security of companies, countries and the world at large**.

1 https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf

Popper's big question is about something more fundamental still. It is about **who we are**. European leaders need to work out what kind of societies they want to protect, cultivate and innovate. In between security, freedom and identity, all kinds of paradoxes arise:

- Must we sacrifice freedom to stay safe?
- If so, are we still the kind of society we want to be?
- Who do we choose to be in the face of these disruptive forces?

It is exactly in times like these that we may remember the genius of Popper, that lays not in his ideal of the open society per se, but in his insistence that we must never take its security for granted, nor fall prey to those prophets who claim to foresee its inevitable demise. Instead, we must innovate our security and revitalize our sense of self. We must, to use Popper's own words:

"[…] go on into the unknown, courageously, using what reason we have, to plan for security and freedom."[2]

This is a **call to action** to do just that: **plan for security and freedom**. In this paper, we'll build our argument along the following lines:

- In chapter 2 we define THE NEW SECURITY NEXUS, which we believe should be the focal point for our security strategy in the coming decades.
- In chapter 3 we briefly explore the impact of DIGITALIZATION.
- In chapter 4 we give an insight in the evolving CYBER THREAT LANDSCAPE.
- In chapter 5 we describe how the context of GEOPOLITICS is evolving.
- This results in chapter 6, where we define the TOUGH QUESTIONS to answer regarding the new security nexus challenges.

2 Popper, The Open Societies and its Enemies, vol. 1, p. 177

Chapter 2
The new security nexus

2.1 A convergence of cycles

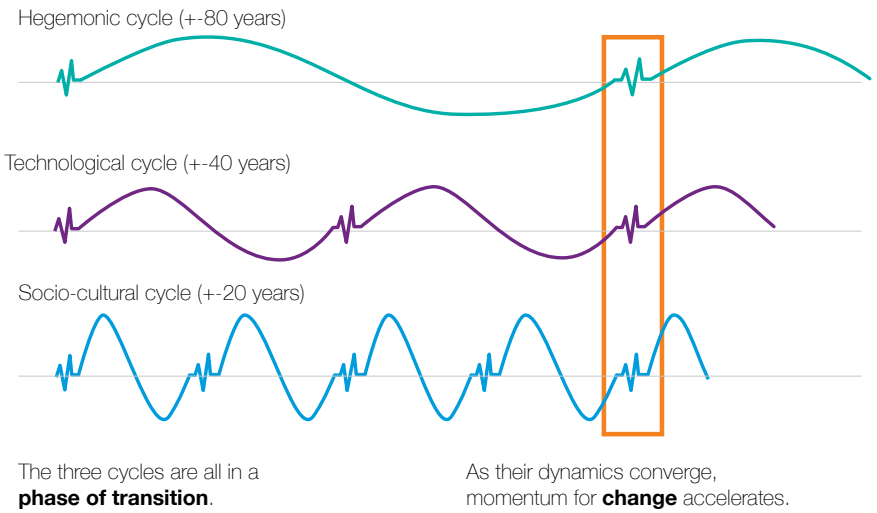
Few would have predicted twenty years ago that GPS systems would be used by nation states for warfare. Few would have considered a scenario where elections were being manipulated by using social media.

Yet, these and other scenarios have unfolded, in fact offering Hollywood producers a wealth of options for dystopian productions. It shows that we live in disruptive times, also when it comes to security. Haroon Sheikh puts the geopolitical and the technological aspects of security disruptions in perspective by pointing out the cycles in hegemonic, technological and socio-cultural change. These cycles tend to follow a pattern:

- every **20 years**, a new generation changes society by pushing new cultural and social values;
- every **40 years**, the workings of our societies and markets change fundamentally by virtue of technological breakthroughs;
- every **80 years**, a new hegemonic power takes the lead in the geopolitical world order.

The exciting thing is that we have entered an era in which all three disruptive cycles are in a phase of transition, **simultaneously**.

Convergence of cycles accelerates change



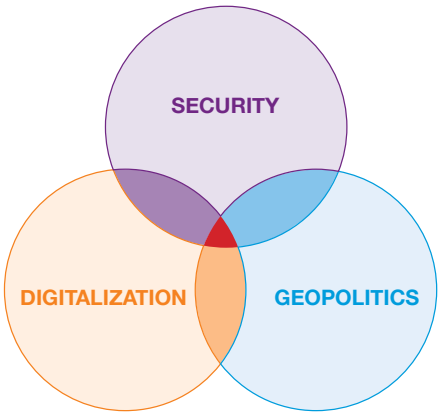
3

3 Sheikh, H. - Cycles and dynamics of change

This causes rapid, large and unpredicted changes. The geopolitical context of security is changing rapidly – as China rises, the US becomes more protectionist, and the EU is struggling to flex its geopolitical muscle – and at the same time the technological base of virtually every form of security infrastructure is going through revolutionary, and often little understood, innovations – from GPS to 5G. When we look at the current controversy regarding 5G and Huawei, we see these three cycles shifting right under our noses. The US and China are aware that who owns the fourth industrial revolution, will probably dominate global networks of power for decades to come, and will be able to push socio-cultural norms regarding freedom of information, privacy and security.

In short, there is no better time to explore the NEW SECURITY NEXUS than right now. It refers to the double disruption of our security that the current technological and geopolitical revolutions add up to. To illustrate:

The new security nexus



The big questions arising in the new security nexus are already dominating public debate. To what extent must Chinese or Russian high-tech companies be allowed to provide elements of infrastructure to European countries? Must Europe try to be a 'strategically autonomous' superpower and would that even be possible? Do hacks by foreign intelligence services constitute 'acts of war'?

2.1 What is security?

So, what do we talk about when we talk about security?

Theoretically, it is not hard to answer this question. Security is the freedom from, or resilience against, potential harm caused by others[4]. Deeper still, security can be said to be *"about survival. It is when an issue is presented as posing an existential threat to […] the state, incorporating government, territory and society."*[5] A person's security can be threatened by real things, like a bullet being fired, just like one can have a sense of

4 https://en.wikipedia.org/wiki/Security
5 Buzan, Waever, De Wilde, Security: a new framework for analysis. https://www.uni-erfurt.de/fileadmin/public-docs/Internationale_Beziehungen/BA_Einfuehrung_in_die_IB/BUZAN%20+%20WAEVER+%20WILDE_%201998_Security_CH%201+2.pdf

insecurity regardless of the objective circumstances – having learned extremely well for an exam, one can still feel insecure about taking it. Security, in the end, is also a social game: security is what people – and states – make of it.

In the **real world**, however, the question of what constitutes a threat and what constitutes security is harder to answer. The emergence of hybrid warfare has made security as an opaque concept.

NATO puts it this way: *"Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations."*[6]

In a way, the concept of hybrid warfare lacks a definition. As a consequence, policy and academic circles have been trying to find a framework for security issues that is comprehensive, integral, as well as practicable. An example of such a framework is put forward by the Dutch National Security Strategy[7], Defense Doctrine[8], and the Comprehensive Foreign and Security Policy Strategy[9].

It defines security as safeguarding six vital interests. These can be adopted to fit the purposes of this paper:

Six vital interest of security	
Aspect	Explanation
Territorial security	The protection of borders
Physical security	The protection of citizens and infrastructure
Economic security	The protection of trade, commerce and industry
Ecological security	The protection of the environment
Social and political stability	The protection of basic values and rights such as the rule of law, democracy and privacy
The functioning of the international rule-based order	The protection of institutions of global governance, upholding international law and safeguarding human rights.

Source: https://www.defensie.nl/downloads/publicaties/2019/06/19/herziene-nederlandse-defensie-doctrine-ndd-2019

6 https://www.nato.int/cps/en/natohq/topics_156338.htm
7 https://www.nctv.nl/binaries/Nationale%20Veiligheid%20Strategie%202019_tcm31-393099.pdf
8 https://www.defensie.nl/downloads/publicaties/2019/06/19/herziene-nederlandse-defensie-doctrine-ndd-2019
9 https://www.rijksoverheid.nl/documenten/kamerstukken/2018/03/20/kamerbrief-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs

Note that all of these vital security interests point to fundamental existential aspects of our societies:

- how we define our borders;
- our personal feelings of safety;
- the way we do business;
- live in harmony with our surroundings;
- and the values we see reflected in local, national and international politics.

2.3 What's at stake?

The new security nexus is about all of these vital interests, in so far as they are challenged by the double disruption of digitalization and geopolitics. It calls for strategic leadership to manage the big security issues of our times, together. That is why the Dutch government proposes a society-wide approach to security, which means that *"governments, security services, military forces, corporations, and NGOs are actively asked to contribute to safeguarding national security."*[10]

Common wisdom has it that you can't solve new problems with old methods. So we will need new strategic leadership to effectively deal with the new security nexus. In fact, every important historical moment is marked by these sorts of shifts to new social models, which expand in velocity and complexity well past what the current ways of thinking can handle. Our predicament is no exception. And usually the source of the **greatest historical disasters** is that so few people at the time either recognize or understand the shift[11]. If any state has learned this lesson, it is China: by failing to understand the new networks, technologies and norms of global security of the mid-19th century, imperial China, as what had been the largest economy in the world for centuries and an untouchable regional hegemon for longer, was largely destroyed by relatively small European powers in a matter of years. We are, once again, on the verge of such a shift.

So, let's dive in to gain more understanding.

10 https://www.rijksoverheid.nl/documenten/rapporten/2019/08/21/ek-bijlage-tk-tegengaan-statelijke-dreigingen
11 Joshua Cooper Ramo, *The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It*

Chapter 3
Anatomy of a new digital reality

3.1 Technology and its two faces

Historically, technology has always had two faces. One is the perspective of progress and innovation. This is also true for the digital transformation in society. The transformation brings us very useful innovations and has opened up societies. However, it also leads to **new vulnerabilities** and may contribute to **shifting powers**. The combination of these two factors may be far reaching, and may also shed a new light on the freedom in our society.

Many of the very first internet users dreamed of an internet which would be unregulated. They envisaged the whole of cyberspace as their independent republic, where governments had no influence. The following is an extract from the beautiful 1996 'Declaration of the Independence of Cyberspace' by the Cyber-Libertarian movement, headed by John Perry Barlow:

> *"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."*[12]

More than twenty years later, we know much better, as the other face of technology has become apparent. Both governments and corporate companies claim their stake in cyberspace which is far from an information Walhalla. Even Barlow himself knows better; in an interview in 2004, he said when asked, *"We all get older and smarter."*[13] Cyberspace is not a free republic (any longer); it has become part of the mainstream world, where laws and regulations play a major role. And where malicious organizations have an impressive array of new options.

12 https://en.wikipedia.org/wiki/A_Declaration_of_the_Independence_of_Cyberspace
13 http://reason.com/archives/2004/08/01/john-perry-barlow-20

As the Minister for Security and Justice F. Grapperhaus writes in a letter to Dutch parliament:

> *"The uncomfortable paradox is that exactly those freedoms that make our open societies possible, at the same time offer malevolent stately actors opportunities to undermine our security and infringe upon our freedom. The openness of our society demands a careful balancing of grasping opportunities and protecting national (security) interests."*[14]

We could refer to the words of the British author C.P. Snow who wrote about the aforementioned faces of technology in 1971.

> *"The only weapon we have to oppose the bad effects of technology is technology itself. There is no other. It is only by the rational use of technology – to control and guide what technology is doing – that we can keep any hopes of a social life more desirable than our own: or in fact of a social life which is not appalling to imagine."*[15]

All of this is especially relevant as developing technology is also key in the power shifts. Throughout history, those who defined the technical standards, ruled the world[16]. In the 19th century the United Kingdom ruled the technical standards and in the 20th century the United States. Even the Netherlands ruled the seas by virtue of its unparalleled skills in maritime engineering during the 17th century. Currently China is taking over this role with their investments in **Artificial Intelligence** and **5G**. China plans to be the leader in AI by 2030 through their 'New Generation Artificial Intelligence *Development Plan'*[17].

The question is: **How do we effectively control and guide what technology is doing, thereby working on a secure society? How do we plan for security and freedom?** In order to answer this question, we must explore both faces of technology.

14 https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2019/04/18/tk-tegengaan-statelijke-dreigingen/tk-tegengaan-statelijke-dreigingen.pdf
15 https://www.nap.edu/read/2129/chapter/22
16 Rob de Wijk – De nieuwe wereldorde
17 The State Council of China - New Generation Artificial Intelligence Development Plan (July 2017)

3.2 The new digital reality

This chapter briefly explores how (digital) technology leads us into a new reality. We limit ourselves to an analysis of three consequences: **hyper connected ecosystems; blurring lines between physical and digital worlds and the impact of algorithms and AI**.

Perspective #1
From splendid isolation to hyper connected ecosystems

Companies now operate in a complex world of hyper connected ecosystems. Competitive advantage is often no longer based on the ownership of certain assets. The source of differentiation (and thereby economic value) rather comes from having access to the assets, by having a solid and strategic position in hyper connected ecosystems. Boundaries between organisations are fuzzy, supply chains are integrated. Even innovation is often a joint process.

The positive effect is that a range of new innovations has unfolded. However, in this hyper connected world, companies have become far more dependent on their partners. In nearly every aspect of their processes.

Perspective #2
Physical = digital

The World Economic Forum coined the term fourth industrial revolution to capture the massive shift in the modern history of the world[18]. In a nutshell: the first industrial revolution involved the mechanisation of production using water and steam. The second was about mass production. The third refers to automation of production, based on new information technology. The fourth is characterised by technologies that start blurring the lines between physical, digital, and biological spheres.

The Internet of Things (IoT) takes a central stage in the fourth wave. Many objects, ranging from cars to buildings and from watches to thermostats, are now connected 24/7. The IoT grows with exponential pace and leads companies into a new reality with massive opportunities. 5G is at the core of this exponential growth, supporting all sorts of devices to connect to the internet at low cost in high density areas. Experts foresee a new range of platform companies based on a maturing Internet of Things. The rationale behind this: powerful platforms such as Uber and Facebook started to blossom when the smartphone was adopted by the mass; a similar pattern may occur for the next wave of platforms in many other sectors, such as logistics, agriculture or banking: they will be turbo-powered by a mature IoT. In other words: IoT is the infrastructure for the next wave of platforms.

18 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Perspective #3
Algorithms guide our decisions

Artificial Intelligence is a game changer in many ways and brings the world innovations in nearly every domain. It accelerates the earlier mentioned fourth industrial revolution, and many companies feel the urge to jump on the bandwagon. This is understandably, as the 'winner takes all' effect may be strong in this domain. First-movers have a strong advantage as they feed their AI systems with sample data sooner than late-joiners. Late-joiners therefore have to go through the full learning cycle themselves, and do not benefit from 'leaked' innovation of first-movers. First-movers have the advantage of providing better services sooner, and thereby are the preferred choice over late-joiners[19].

The rise of AI also has another effect. The algorithms that are at the core of this technology guide us through many decisions, both in personal lives as in business and politics. In line with Lawrence Lessig's famous essay 'Code is law'[20] – in which he argued that software increasingly dominates our behaviour – we start to experience how machines take over not only operational human tasks but also automate decisions and even the work of managers.

Prominent thinkers also point out to us the dangers of abusing algorithms for bending public and political opinions. Evgeny Morozov talks of 'invisible barbed wire'[21] that guides us without us knowing. The software coders indeed have more influence than ever before.

One important aspect to take into account is that people generally trust algorithms without giving it much thought. By default, we believe machines are 'more honest' than humans. This blind faith is precisely the reason why we need to ensure that algorithms work well 'under the hood'. Another aspect is the fact that large tech (platform) companies become more powerful because of this development. Via their algorithms, they gain power to influence the decisions of millions of people, as we have seen in the Cambridge Analytica scandal.

19 VNO-NCW – AI voor Nederland: vergroten, versnellen en verbinden https://www.vno-ncw.nl/sites/default/files/aivnl_20181106_0.pdf
20 Lawrence Lessig – Code is Law
21 Evgeny Morozov – The Real Privacy Problem

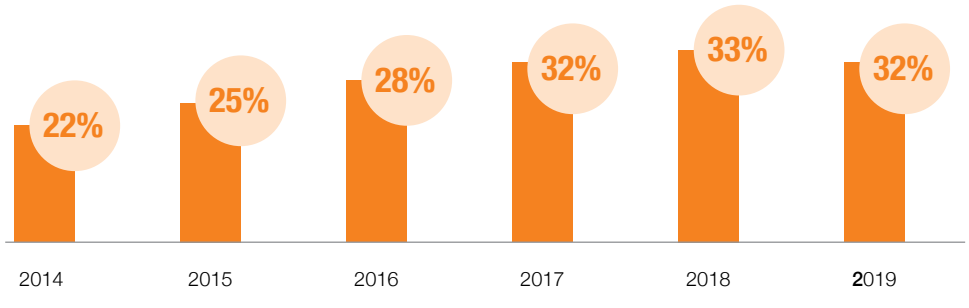
Chapter 4
Spotlight on emerging threats

As we have seen in chapter 3, technology alters our society in a rather fundamental way. To fully understand what is at stake in terms of security, we will now explore how new threats emerge and how we should deal with these new threats. We will do this in three perspectives. First we will explore the changing (definition of) vital infrastructure (4.1), followed by an analysis of how attackers and their weapons evolve (4.2). We conclude with an analysis of how lines are blurring between friends and enemies (4.3).

4.1 Business as usual

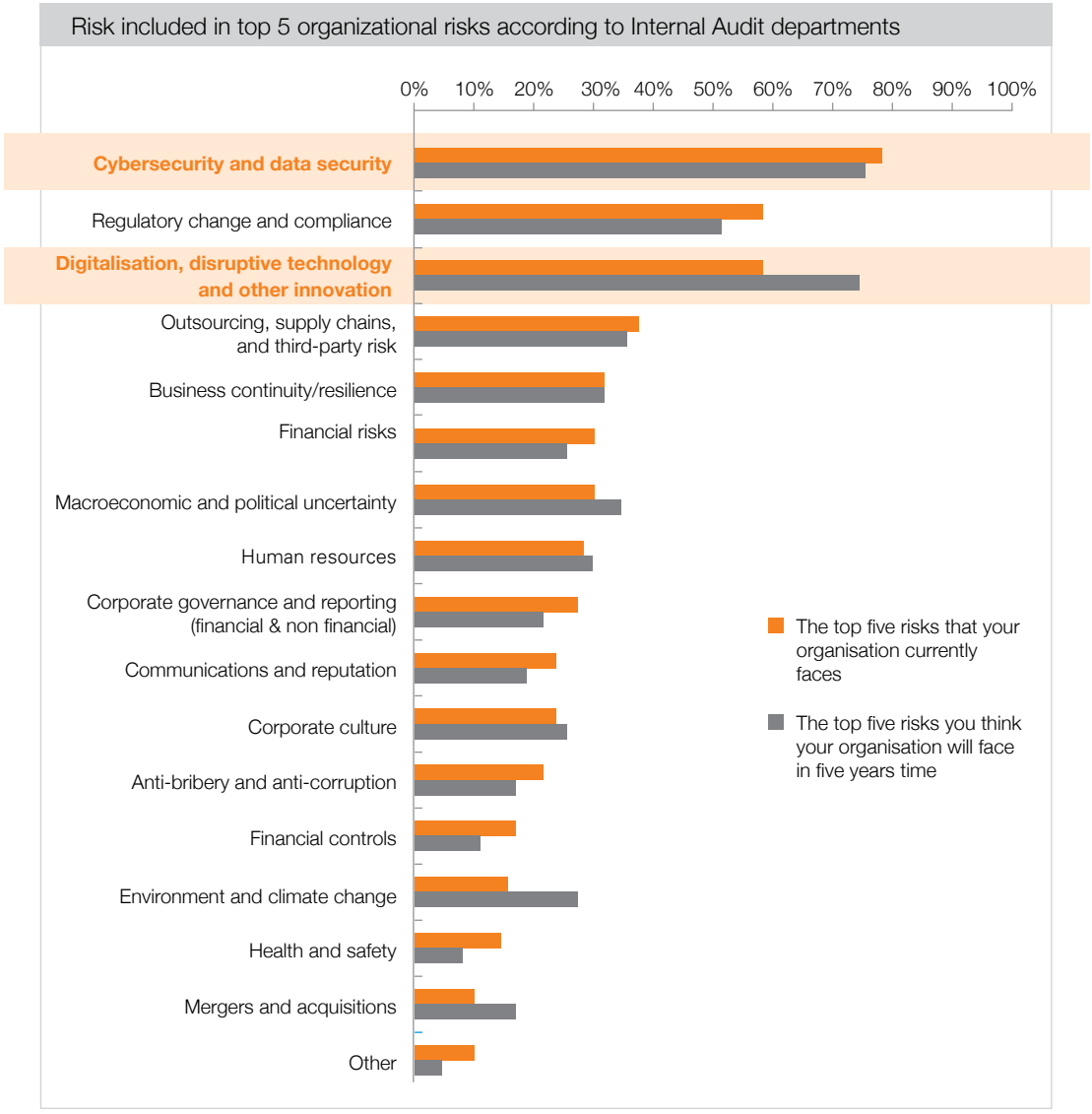
Many leaders in both the private and public sector fully understand the importance of cyber security for their business outcomes and objectives. The stakes are high. Not only in terms of the risk of interruption of vital services following attacks by malicious groups, but also in terms of digital espionage or theft of intellectual property. Experts estimate that **commercial espionage** may endanger economic growth to an amount of **55 billion** euros and up to **289,000 jobs in the EU**[22]. According to a global survey by Harvey Nash and KPMG, held with over 3,500 Chief Information Officers (CIOs) in over 100 countries, 32% experienced a major cyber-attack in the past two years (only 22% in 2014)[23]. According to a survey from the Institute of Internal Auditors held under Chief Audit Executives across Europe about the biggest risks to their organizations, 78% put cyber security and data privacy in their top 5 risks and 58% put digitalization, disruptive technology and other innovations in their top 5. Asked about these risks in five years' time, a sheer 75% put both cyber security and digitalization in their top 5[24].

Number of CIOs that reported experiencing a major cyber-attack in the past two years



Source: KPMG / Harvey Nash – CIO survey 2019

22 Hosuk Lee-Makiyama - Stealing Thunder: Cloud, IoT and 5G will Change the Strategic Paradigm for Protecting European Commercial Interests. Will Cyber Espionage be Allowed to Hold Europe Back in the Global Race for Industrial Competitiveness?
23 KPMG/ Harvey Nash – CIO survey 2019 https://home.kpmg/nl/nl/home/insights/2019/06/a-changing-perspective.html
24 https://www.iia.nl/SiteFiles/Publicaties/Risk%20in%20Focus%202020%20IIA%20NL%20LR%20def.pdf



Source: Source: The Institute of Internal Audit – Risk In Focus 2020: Hot topics for internal auditors

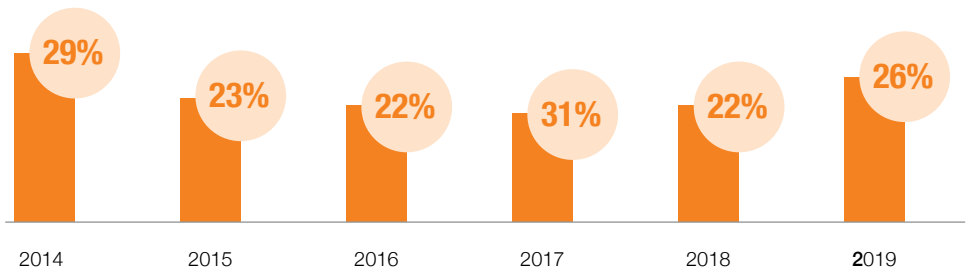
What is the best attitude toward this emerging threat?

Acting out of fear is probably not the best option, although it has been the strategy of many cyber-related companies who use the concept of Fear, Uncertainty and Doubt (FUD) for marketing their services, drawing on prevailing incidents in the media.

Unplugging the cables by not jumping on the bandwagon of new digital opportunities is also not a serious option, as it would stifle innovation completely and paralyze economies. It is simple: You can't **unscramble eggs**.

So the only viable option is to deal with the threats by considering it as 'business as usual' and building a risk management approach. This starts with recognizing what is at stake – the 'crown jewels' – and analyzing which parties should be monitored closely. Only then can we align security strategies on this analysis. In the light of the aforementioned new reality (chapter 3) we will dig into some new vulnerabilities for society in this chapter. Fortunately, according to the same survey by Harvey Nash and KPMG, more and more CIOs feel they are very well prepared for attacks (26%, compared to 21% in 2017). Which is in contrast to the results of The Netherlands Scientific Council for Government Policy Research on Preparing for Digital Disruption[25]. This research indicates that most implemented cyber-security measures in Dutch companies and government bodies are related to prevention of cyber-attacks rather than to prepare for one (detection and response). **Are CIOs mixing up prevention with preparation?**

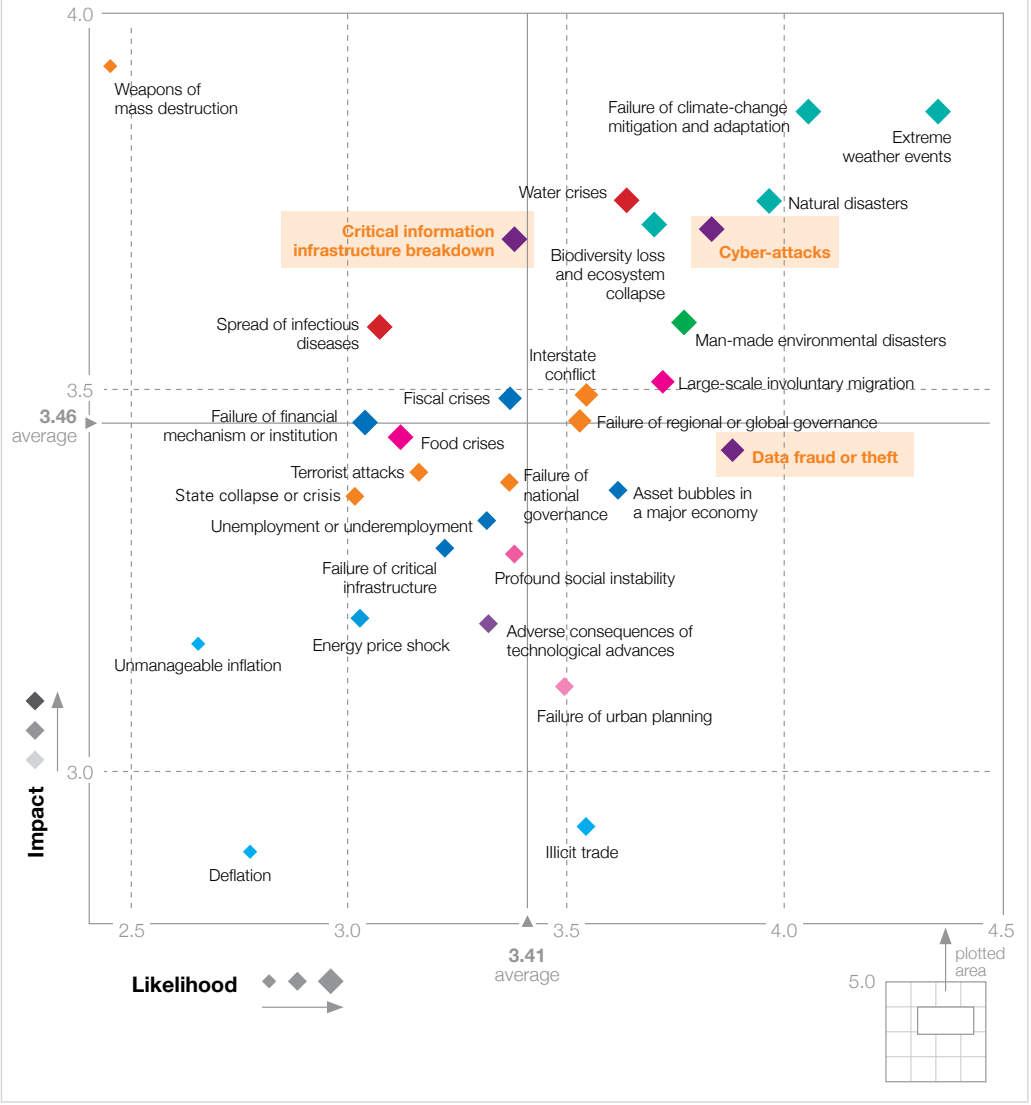
Number of CIOs that report feeling very well prepared for cyber-attacks



Source: KPMG / Harvey Nash – CIO survey 2019

25 https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

Top risks according to World Economic Forum



Source: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

4.2 Social dependency on digital backbones

It is also important to understand the risks of social disruption. The work of The Dutch National Coordinator for Security and Counterterrorism, gives insight in the critical infrastructure and processes in the Netherlands[26]. These infrastructures and processes are of vital interest to society and incidents pertaining to these may cause social disruption. Their criticality is split into two categories, depicted in the table below.

26 https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

Critical infrastructure categories in the Netherlands		
	Category A	Category B
Economic impact	More than 50 billion euros or 5% loss of GDP	More than 5 billion euros or 1% loss of GDP
Physical impact	More than 10.000 people dead, severely injured or chronically sick	More than 1.000 people dead, severely injured or chronically sick
Social impact	More than 1 million people suffer from emotional problems or serious societal survival problems	More than 100.000 people suffer from emotional problems or serious societal survival problems
Cascade impact	Impact cascades to at least two other infrastructures or processes	

Source: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

New vital services

In order to assess what is at stake in terms of security, we must obtain a clear view on the 'new' digital backbones of vital infrastructures and processes that may be at risk in terms of social disruption. A newly ratified EU legislation (Wet Beveiliging Netwerk- en Informatiesystem (WBNI))[27] defined an interesting set of 'critical industries'. On the one hand that consists of vital service providers (e.g. energy, financial and transport sector) – the 'usual suspects'; on the other hand the definition includes digital service providers (e.g. cloud providers, online search engines and online marketplaces). The latter category is "although not vital, they are very important: many citizens/customers and companies use their services or are dependent on their services." The WBNI mentions , however, also some interesting new players that are of vital importance for our digital backbone:

- internet hubs such as the Amsterdam Internet Exchange;
- providers that manage a minimum of 1 million top level domain names[28];
- providers that manage the Domain Name System for a minimum of 1 million top level domain names[29].

27 https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners
28 Top level domain names are websites that end, for example, with a country code (www.nos.nl or www.diezeit.de)
29 Domain Name Systems are the routing software on the internet, they tell us where we can find the exact computers behind top level domain names (e.g. the exact computer where the content of www.nos.nl can be found)

Awareness

The European Union and the Netherlands demonstrate increasing awareness for the impact of disruption of important digital backbones. The World Economic Forum coined cyber-attacks, critical information infrastructure breakdown, data fraud and theft in their top risks of the Global Risk Landscape 2019[30].

To gain understanding of the impact of such disruptions, we illustrate two cases.

CASE STUDY #1

Public Key Infrastructure: an attack on the 'trust tree'

Many of us remember how a Dutch company, Diginotar, was hacked in 2011. This company played a crucial role on the internet. Put simply, any website that provides a secure connection (e.g. for internet banking) shows a green 'lock' in the internet browser. That lock indicates that another company confirms the security of that website (trust). Via a complex tree structure of trust we end up at the top with a few main companies that all internet browsers trust. Diginotar was one of them. When Diginotar was hacked, the complete internet trust tree structure was broken: the hacker set up a fake branch in that tree and was able to set up fake websites that seemed trustworthy. Iranian national hackers thereby intended to let Iranian internet users log on to a set of fake websites technically put in front of the real websites. In the end, they were able to let internet users log on to a fake version of, for example, Gmail (Google mail) and steal their passwords. They very likely ended up prosecuting people based on the content of their mailbox. This hack showed the weakness of that internet trust structure and the impact of a hack through just one player in that trust tree[31].

30 http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
31 This case is very well documented, but especially well in the book by Huib Modderkolk – Het is oorlog maar niemand die het ziet

CASE STUDY #2

GPS: faking geographic positions

Yet another example where Iran was involved is much more recent. In the summer of 2019, Iran likely (this is still unproven) persuaded a British oil tanker to sail into Iranian waters. The British were misled by fake GPS signals – they were not aware that they were in Iranian waters – and Iran was able to capture the oil tanker while not leaving their own waters[32].

GPS is known to have severe technical weaknesses as it can not be protected against fake signals or against being completely jammed (i.e. no signal coming through). Alternatives are in the making, and it looks like China's BeiDou has the best cards to win this game[33]. The difference between the Chinese BeiDou and American GPS is the fact that BeiDou operates a two-way communication system. This means that China might be able to determine the location of those retrieving their own location, plus they might be able to shut down their services locally. Currently, BeiDou outperforms GPS in many geographically interesting areas to China and many devices (e.g. smartphones) from Chinese companies already have a BeiDou chip built-in by default.

All of this is particularly relevant given the fact that the United States Department of Homeland Security has found that 15 out of 18 of their Critical Infrastructure and Key Resources have some degree of dependency on GPS (especially timing based on GPS)[34].

4.3 The changing face of cyber weapons

Attackers

The nature of cyber-crime continues to evolve. In fact, it has democratized: in this digital world, everyone has seamless and unlimited access to information and (training) resources to become a hacker[35].

We can roughly categorize the attackers:

Most hackers are referred to as '**scriptkiddies**' (i.e. inexperienced, usually young adolescent individuals executing attacks (scripts) they found online without deep technical knowledge). The impact of their cyber-attacks is, however, not to be underestimated.

32 https://www.mirror.co.uk/news/world-news/iran-tanker-crisis-mi6-probe-18458279
33 https://asia.nikkei.com/Business/China-tech/China-s-version-of-GPS-now-has-more-satellites-than-US-original
34 https://www.gps.gov/multimedia/presentations/2012/10/USTTI/graham.pdf
35 https://www.thehaguesecuritydelta.com/media/com_hsd/report/225/document/ecsp-2019-european.pdf

In the Netherlands we have experienced their social impact by cyber-attacks on the availability of online banking infrastructures of ING Bank and ABN AMRO in 2018, and the digital penetration of the KPN network in 2012[36]. These scriptkiddies are motivated to attack merely for fun, or because they don not agree with a certain government or corporate's view.

Another important category of digital threat actors are **cyber-criminal gangs**, especially from Russia and former Soviet states. These gangs have gone through a high maturity journey to mimic real companies. In the digital underground, these gangs sell e.g. cyber-crime consultancy services, inbound callcenter calls for viruses they have sold or do translation work for phishing e-mails[37].
They are all purely financially motivated and it is expected that the first of these cyber-criminal gangs is earning more than 1 billion euros in 2019. An interesting example is the Carbanak hacker group that was allegedly able to hack certain banks in Europe and have ATMs spit out money of accounts of which they had manipulated the content[38].

Last but not least, **nation state actors** have entered the cyber-crime arena. Ever since Edward Snowden, former NSA contractor, revealed the depth and techniques used by the United Sates, it has become clear how much nation state actors invest in dominating the digital world. Most focus on digital espionage and anti-terrorism. The Dutch secret service specifically mentions China, Russia and Iran as nation states that have an active cyber program aimed towards the Netherlands[39].
An interesting example related to these actors is the public announcement of the Dutch Military Intelligence Services interrupting a hack by the Russian Secret Service on the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague[40].

Weapons

Broadly speaking, there are two different types of cyber weapons: those that exploit technical weaknesses in the victim's digital infrastructure; and those that merely cause a traffic jam on the internet towards the victim (often called DDoS).

The first category is the more interesting in the context of this paper.

36 Huib Modderkolk – Het is oorlog maar niemand die het ziet
37 https://www.bbc.com/news/technology-48294788
38 https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
39 https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019
40 https://www.rijksoverheid.nl/actueel/nieuws/2018/10/04/mivd-verstoort-russische-cyberoperatie-bij-de-organisatie-voor-het-verbod-op-chemische-wapens

Essentially, these weapons aim to use computer code to exploit technical weaknesses on the victim's digital infrastructure. Some of these weaknesses are known and could have been resolved (e.g. by updating the system), whereas others are only known to the attacker. Those unknown weaknesses are called **Zerodays** (there have been zero days since this weakness is known).

Zerodays are in fact the equivalent of digital diamonds: hard to find and worth a lot.

They are aimed at commonly used systems (such as Microsoft Windows) and are sold on the black market for **more than 1 million US dollars**[41]. Several companies specialize in the trade of these cyber weapons, making millions of euros[42]. Some have been caught selling such weapons to dubious countries[43]. This trend has come to the attention of politicians and some of them argue that these deals be placed under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies[44].

Deploying or using a cyber weapon can be done in high anonymity, making it difficult to trace the origin of the cyber-attacks (attribution), and a good deterrence strategy even more difficult. Following the previously described attack on the OPCW, the Netherlands caught Russia red-handed and chose to announce their capture in public[45]. This 'deterrence by signalling' will likely become the predominant strategy[46].

Deploying a cyber weapon can cause heavy collateral damage: the computer code to exploit the technical weakness reveals this technical weakness and allows others to copy and deploy their own attacks using this weakness. The hacker group 'The Shadow Brokers' posted a Zeroday owned by the NSA ('eternal blue') in public, which was the basis for one of the largest virus attacks the world has ever seen: Wannacry, likely to have infected 230,000+ computers in at least 150 countries and causing approximately 4 billion US dollars in financial losses[47]. **The fact that the NSA did not report this technical weakness raises questions to their role as security service**.

41 https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/
42 https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/
43 https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027
44 https://www.tandfonline.com/doi/abs/10.1080/19331681.2019.1616646
45 https://www.defensie.nl/actueel/nieuws/2018/10/04/mivd-verstoort-russische-cyberoperatie-bij-de-organisatie-voor-het-verbod-op-chemische-wapens
46 https://www.clingendael.nl/sites/default/files/Cyber_Deterrence.pdf
47 https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later

Geopolitical use of cyber weapons

Cyber weapons are also frequently deployed in geopolitical conflicts. The motives behind these attacks vary.

Some attacks aim for financial gains. The People's Republic of Korea (North Korea) has, allegedly, gained over 2 billion US dollars by cyber-attacks on the financial industry to fund their Weapons of Mass Destruction programmes[48].

Another category involves disrupting the enemy. We have for instance witnessed how Iran attacked the Saudi Arabian Oil Company (Saudi Aramco) in 2012, wiping the hard disks of 30,000 computers[49]. Another example is Stuxnet[50], a virus that aimed to disrupt the Iranian nuclear programme in Natanz. According to Volkskrant-journalist Huib Modderkolk, the virus was deployed with the help of an Iranian national recruited by the Dutch General Intelligence and Security Services[51].

These cyber weapons can also be a means to gain political influence. Hackers of the Russian external intelligence agency SVR (going by the name Cozy Bear) have been accused of attacking the United States Democratic National Committee in 2015 to influence the 2016 elections. According to Huib Modderkolk, the Dutch General Intelligence and Security Services have played a major role in discovering the attack and informing the United States[51].

Closely related to this is gaining intelligence. Edward Snowden, former NSA contractor, and website Wikileaks have uncovered many intelligence operations from the United States and the United Kingdom. Cases included spying on Belgian telco Belgacom and German prime minister Merkel.

Last but not least, cyber weapons can be deployed for hybrid warfare. Conflicts between states take place largely below the legal threshold of an open armed conflict, with the integrated use of means and actors, aimed at achieving certain strategic goals[52]. These means frequently include cyber weapons or fake news[53]. The aforementioned Stuxnet case is an example of this, as is the example of the United States deploying targeted killings using drones on suspects of terrorism. The Dutch Military Intelligence

---

[48] https://undocs.org/S/2019/691
[49] Bronk, C., & Tikk-Ringas, E. (2013). Hack or attack? Shamoon and the Evolution of Cyber Conflict
[50] Zetter, K. (2014). Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon
[51] Huib Modderkolk – Het is oorlog maar niemand die het ziet
[52] https://www.nctv.nl/binaries/nctv/documenten/kamerstukken/2019/04/18/kamerbrief-tegengaan-statelijke-dreigingen/TK+brief+Tegengaan+statelijke+dreigingen.pdf
[53] https://www.clingendael.org/sites/default/files/2018-05/Report_Hybrid_Conflict.pdf

has, according to Huib Modderkolk, supplied the United States with telecom intel from a Dutch marine vessel equipped with specialized NSA equipment. This intel is used to conduct targeted killings with the help of the location of SIM cards, blending conventional weapons with cyber intelligence [50].

4.4 Blurring lines

The face of (cyber) security is also changing in another perspective. In the traditional perspective on security, one would know who the players were and how their relationship with other parties was. In the digital era, this has changed. The lines are blurring between three perspectives:

Perspective #1
Coalitions are multidimensional: friends may be part-time enemies

The rise of digital technology provides extremely cost-efficient means to build intelligence and offensive capabilities. Whereas this used to be an exclusive domain for superpowers, nowadays this has evolved into a level playing field. The new dynamic is that everyone spies on everyone.

One of the effects is that stable long-term partnerships turn into multidimensional coalitions. States may work shoulder to shoulder in a trusted relationship on one strategic goal, while they may treat the same state as an enemy in other areas. It may well be possible that good friends indeed penetrate each other's infrastructure. As an example, the solid relationship between the United States and Israel has been put to the test at least twice in the cyber domain:

- Israel has been accused of deploying very sophisticated malware against Swiss hotels where the P5+1 conversations were on the Iranian nuclear deal between US, UK, Germany, France, Russia, China and the EU with Iran[54].
- Recently, Israel has been accused of deploying sophisticated devices near the White House to spy on cellular networks likely used by Trump and his staf[55].

54 https://www.theguardian.com/technology/2015/jun/11/duqu-20-computer-virus-with-traces-of-israeli-code-was-used-to-hack-iran-talks
55 https://www.theguardian.com/world/2019/sep/12/israel-planted-spying-devices-near-white-house-says-report

Perspective #2

Private morphs into public; large corporates may even have more influence than governments

Collusions between commerce and power have been a fact of life throughout history. The digital transformation of society has added new dynamics to this. Collaborations between state and non-state actors on cyber espionage are common practice, especially in China and Russia. One important factor is that nearly all digital infrastructure is owned by commercial actors, giving these companies extensive power and making governments dependent on them.

Another important factor is the sheer power that some large tech companies have because of the size of their customer base. Successful platform models are built on massive volumes and on the fact that these platforms have a central place in an ecosystem to create value. This gives them the power to not only dominate markets but also to influence opinions or to infringe on (personal) data on a large scale. A sign on the wall is that the largest five technology companies in the US are sometimes dubbed 'the frightful five'.

The differences between the US, China and Europe become clearer over the years and are a decisive factor in the influence that companies have. Private sector-led innovation predominates in the US. The European Union gives priority to citizen and consumer rights, which may put pressure on competitiveness. China typically has state-backed technological competition in which the government has more access to citizens' data.

Perspective #2

Breaches and espionage may be untraceable for long time: who looks like a friend may be an enemy under the radar

One of the differences between physical security and digital security is that in the latter case, there often are no 'smoking guns'. Attackers can penetrate systems and infrastructures unnoticed. Their addresses can be cloaked or falsified. In other words: states who believe that another state is a friend may in fact already be infiltrated by that very same state or be 'at war' under the hood.

This also means that it is hard to assess the follow-up of international signatories agreed not to engage in commercial espionage. Experts argue over the effectiveness of the agreement between China and the US. Some believe it is effective in combating espionage. Others claim the opposite, as it is easy to cheat on the agreement because there are few means of detection.

Chapter 5
The transformation of global power and why it matters to security

It is not yet clear who will dominate the new security nexus. The race is on and it already raises fundamental strategic questions about European security. It is a matter of understanding how the nature of global power is shifting. In a horizontal manner from the West (the US) to the East (China). And in a vertical manner, from states to global, digital networks.

5.1 Black swans and grey rhinos

Perhaps no world leader understands this better than President Xi Jinping of China. He spoke of two threats to his country's power: grey rhinos and black swans.

> *"[We are] confronted with unpredictable international developments and a complicated and sensitive external environment. […] We must maintain a high degree of vigilance. We must keep our high alert about any 'black swan' incident, and also take steps to prevent any 'grey rhino' threat."* [56]

Xi Jinping refers to the grey rhinos as "highly probable, high impact yet neglected threats" according to author Michelle Wucker[57], who coined the term. Climate change can be said to be a grey rhino. He also refers to the black swans, as popularized by investment banker and philosopher Nicholas Nassim Taleb[58]. These are events that no one is able to predict but have a revolutionary impact on the world. The 2008 financial crisis is a prime example of a black swan.

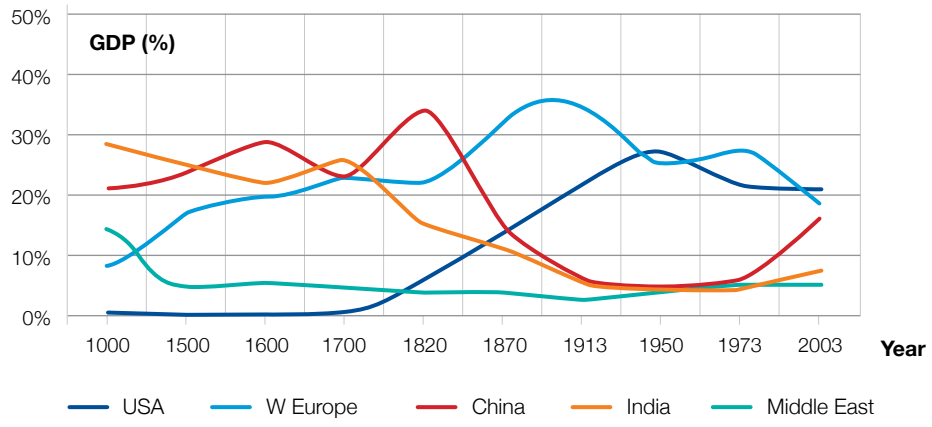
With these concepts, the Chinese president points out that the power balance is transforming in two directions at the same time. On the one hand, there is a grey rhino power shift from West to East (the US to China), which has long been neglected by European leaders. On the other hand, there is a black swan shift from states to global digital networks, as a result of globalizing trade and information networks. Any successful leader will have to manage both.

56 https://www.scmp.com/news/china/politics/article/2183067/be-vigilant-about-threats-chinas-stability-and-reforms-xi
57 Michelle Wucker – The Gray Rhino
58 Nicholas Nassim Taleb – The Black Swan

5.2 Belt and Road Initiative: Marco Polo reinvented

Many of us see Marco Polo as a symbol of the historic successes of European commerce. In reality of course, Polo was symptomatic of the pull of the East, and in particular the markets and civilizations of the Asian Silk Road – a bustling chain of deeply connected trade hubs ranging from Constantinople to Beijing. Closely related to that: the Western geo-economic dominance has been but a blip in world history. The leading British economic historian Angus Maddison published studies based on vast quantitative analyses that confirm this.

Historical trends in global distribution of GDP in China, India, Western Europe, the US and the Middle East



59

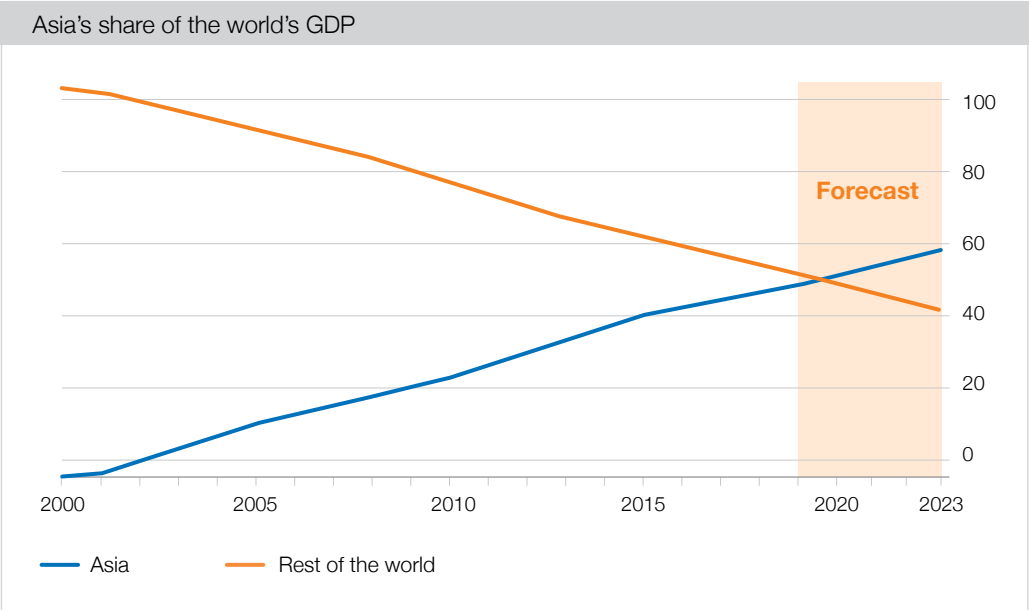
Source: https://upload.wikimedia.org/wikipedia/commons/9/9d/1_AD_to_2003_AD_Historical_Trends_in_global_distribution_of_GDP_China_India_Western_Europe_USA_Middle_East.png

That blip is now over. The future of global commerce and power lies in the East. In other words: Marco Polo's world is making a comeback[60]. In economic terms, the 'Asian Century' begins in 2020, showing that Asia's share of world GDP will then be bigger than that of the rest of the world[61].

That sounds impressive, and it is: in 2000 Asia only counted for a third of world output.

[60] Robert D. Kaplan – The Return of Marco Polo's World.

[61] https://www.ft.com/content/520cb6f6-2958-11e9-a5ab-ff8ef2b976c7



61

Source: https://www.ft.com/content/520cb6f6-2958-11e9-a5ab-ff8ef2b976c7

China becomes the nerve-centre of a new period of global connectivity by virtue of its Belt and Road Initiative. In fact, the transformation is on the same level as what happened in the decades that followed the crossing of the Atlantic by Columbus and the near-simultaneous opening up of trade routes between Europe, the Indian Ocean, South Asia and beyond.

When it comes to leveraging growth to fuel geopolitical power, China is indeed running the game. The impact of the Belt and Road Initiative in this respect, can hardly be overstated: it is quite simply the largest free-trade offensive in world history. The bare facts (see text box) are astonishing:

Belt and Road Initiative (BRI), the facts

Only six years after it was launched, it now encompasses over 1 trillion US dollars in investments.

1 trillion US dollars roughly equals Dutch GDP[62], net worth of Apple[63], Amazon or Microsoft[64], twice the EU Connectivity Strategy65 and ten times the US Marshall Plan[66].

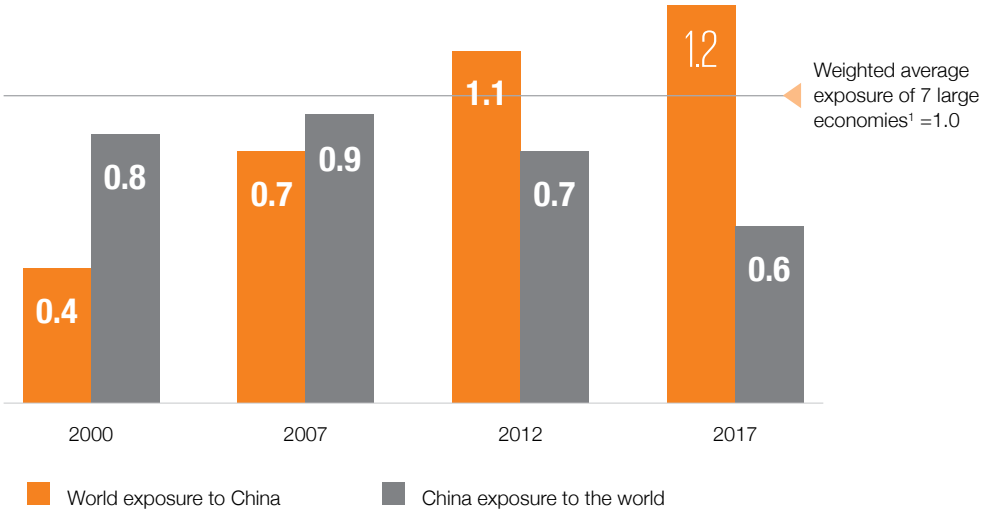
China is investing in all kinds of trade infrastructure, such as dry-ports, shipping routes and railways. It does so in more than 60 countries, in every continent, representing over two-thirds of the world population, covering land, sea and even cyberspace[67].

Most of China's investments go to Western-Europe, but since BRI, Central, Eastern and Southern Europe have been getting a lot of attention from China[68]. *Examples of investments are: financing a 1.1 billion US dollar railway between Budapest and Belgrade; buying a major stake in the Port of Piraeus; sign up of Italy as a BRI-partner, the first belonging to the G7; and setting up the 16+1 Platform – a diplomatic forum to engage Central and Eastern European states outside of the EU's reach.*

China is using BRI to **game globalization**, making the world's economy more exposed to Chinese capital, whereas at the same time China's economy becomes less open to the world.

63 https://www.nbcnews.com/tech/tech-news/apple-worth-1-trillion-here-s-what-much-money-could-n897511
64 https://www.theverge.com/2019/4/25/18515623/microsoft-worth-1-trillion-dollars-stock-price-value
65 https://eeas.europa.eu/sites/eeas/files/joint_communication_-_connecting_europe_and_asia_-_building_blocks_for_an_eu_strategy_2018-09-19.pdf
66 https://www.nytimes.com/interactive/2019/01/29/magazine/china-globalization-kazakhstan.html?mtrref=www.google.com&gwh=3DE54DCFDD2AD4CF5A7FCCB0BAB029C7&gwt=pay&assetType=REGIWALL
67 https://www.economist.com/china/2018/05/31/china-talks-of-building-a-digital-silk-road
68 https://carnegieendowment.org/2018/10/19/europe-s-emerging-approach-to-china-s-belt-and-road-initiative-pub-77536

China has been reducing its relative exposure to the world while the world has been increasing its exposure to China



1 China, France, Germany, India, Japan, United Kingdom and United States

69

Source: McKinsey Global Institute analysis

5.3 BRI and the impact on security

The BRI is not just about gaming free trade. The BRI has a significant security component, as the leading European think-tank MERICS argues: "In 2015, China adopted an anti-terrorism law allowing for foreign missions of PLA units, and it opened its first overseas military base in Djibouti, a hub of the Maritime Silk Road. A new industry of Chinese private security companies is rapidly developing, providing protection to BRI projects. Beijing also touts its technological, law enforcement and military capabilities to countries covered by the BRI on security-related issues like satellite navigation, disaster management and combating crime."[70]

69 https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx

70 https://www.merics.org/en/bri-tracker/mapping-the-belt-and-road-initiative

BRI already buys China **geopolitical influence in Europe, as we have seen a number of times**:

- After China invested in Piraeus, Greece blocked an EU statement at the UN, criticizing China's human rights record – the first time the EU failed to make such a statement.
- Hungary refused to sign a letter denouncing the torture of lawyers in China.
- Hungary and Greece together sought to block any reference to China in an EU statement about the ruling by the Permanent Court of Arbitration in The Hague that struck down China's legal claims in the South China Sea[71].
- Montenegro, candidate to the EU, expected to join in 2025, is running the risk of falling into a so-called 'debt-trap', as it received almost 1.3 billion euros in loans from China to finance a new highway, sending the country's debt from 63% up to 80% of GDP. As the Financial Times writes, *"If Montenegro were to default, the terms of its contract for the loans even give China the right to access Montenegrin land as collateral."*[72]

The BRI is **reshaping geopolitics beyond China**. In Europe, the EU Connectivity Strategy was announced by EU Commissioner Mogherini, although it is not yet clear what the exact size of its budget will be. The EU has signed a free-trade deal and an infrastructure pact with Japan, backed by a 65.48 billion US dollar fund[73]. Russia has launched its own Greater Eurasian Partnership strategy, but lacks the resources to really make it worth it's while. Actually, it has accepted the BRI as an opportunity; not just for economic gains, but also to align itself with the new superpower China. India has serious objections to the BRI, especially to the China-Pakistan Economic Corridor project, which is one of the biggest projects within the BRI, that runs through the disputed territories of Kashmir. It has pushed India to collaborate more closely with its neighbours and Japan[74]. In April of 2018, all EU member states' ambassadors to Beijing (except Hungary) signed a statement saying that the BRI "*runs counter to the EU agenda for liberalizing trade and pushes the balance of power in favor of subsidized Chinese companies.*"[75] This reflects a growing European awareness that China's economic expansion is not just about growth: it is about reshaping global power.

Moreover, when we look more closely at the full-out trade war between China and the US, we will note that this **trade war isn't about trade – it is about dominating the new networks of power**.

---

71 https://carnegieendowment.org/2018/10/19/europe-s-emerging-approach-to-china-s-belt-and-road-initiative-pub-77536
72 https://www.ft.com/content/d3d56d20-5a8d-11e9-9dde-7aedca0a081a
73 https://www.dw.com/en/eu-japan-take-on-chinas-bri-with-own-silk-road/a-50697761
74 https://carnegietsinghua.org/2019/04/25/how-are-various-countries-responding-to-china-s-belt-and-road-initiative-pub-79002
75 https://carnegieendowment.org/2018/10/19/europe-s-emerging-approach-to-china-s-belt-and-road-initiative-pub-77536

In fact, if the trade war were really been about trade, it would have long been over. China has offered on multiple occasions to seal a deal by buying more soybeans and US-made cars – industries that are of vital importance to Trump supporters. However, the trade war has evolved into something much bigger: a struggle for geopolitical dominance between two superpowers, one ruling, one rising.

This in and of itself poses a serious security threat to Europe. Military war almost always accompanies the kind of hegemonic shifts that Haroon Sheikh refers to[76]. The shift of power between the US and China certainly runs the risk of ending in military conflict: disputes concerning the South-China Sea continue to lead to military tensions between the two superpowers, with the potential risk of European countries being dragged in. The Chinese Defence Minister has confirmed what many American commentators have long feared: that China will use BRI to spread its military influence across the globe[77].

The struggle for power between the US and China is not just about military dominance in the classic sense of the word. It is (also) about dominating the new networks of power that are associated with new digital reality – and the fourth industrial revolution that is part of this reality – that we touched upon in chapter 3. The digital revolution has been transforming information flows and is blurring the traditional lines between public and private. It is important to point to China's Made-in-China 2025-strategy (MiC25), which is China's blueprint for becoming a "global manufacturing", "cyber", and "science and technology innovation superpower". China is aiming to achieve this by investing heavily in R&D (China's spending has already surpassed that of the EU, as percentage of GDP), centrally coordinating private and public sector innovation, and creating global leaders in the core-industries of the coming decades.

This is how China is trying to own both power shifts: one the one hand it is using its economic growth and push for global connectivity to fuel its geopolitical rise, and on the other, it invests in those technologies that are not just vital for China's growth, but also for virtually all big security-issues in the coming decades. The AI arms race, to name just one aspect of this, is already under way. NATO recently released a paper which lay the framework for defensive AI agents, which patrol friendly systems and detect enemy malware[78]. The US military has tripled its budget for military-AI, in a clear reaction to Chinese investments in the same are. But, as Lt. Gen. Jack Shanahan says, China has

76 Allison, Graham – Destined For War: Can America and China escape Thucydides' Trap? http://eng.mod.gov.cn/news/2019-07/08/content_4845385.htm
77 http://eng.mod.gov.cn/news/2019-07/08/content_4845385.htm
78 https://www.wired.co.uk/article/artificial-intelligence-weapons-warfare-project-maven-google-china

a leg up, as it is able far more easily to put the resources of private companies and academia to military use: *"If we don't find a way to strengthen those bonds between the United States Government, industry and academia, then I would say we do have a real risk of not moving as fast as China."*[79]

5.4 Europe seems to be stuck in the middle in the new security nexus

The trade war, and especially the conflict over 5G, forces Europe to choose between the economic gains of cooperating with China and its military dependence on the US. At the same time, the technology race pushes new norms concerning security, economics and geopolitics. Europe is trying to adapt, as well as asking itself whether it wants to adapt.

The question is: How will Europe manage in between Trump's America First-policy and Xi's Chinese Dream? These seem to be the new rules of the game:

Embrace geopolitics

New EU-commissioner Ursula von der Leyen has called her new commission the "Geopolitical Commission", clearly indicating that she will take a leading role in coordinating European policy in relation to the US and China. Still, it is as of yet unclear what this will mean in concrete power-political terms. How will she make good on her promise? And what will that do to Europe's image as a "soft power union"?

? Will the new Commission push for higher defence spending by its member states, raising it to 2%, or perhaps even to 3% or 4%? Will it be able to convince member states of the geopolitical importance of the enlargement to the Balkans?

79 https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1949362/lt-gen-jack-shanahan-media-briefing-on-ai-related-initiatives-within-the-depart/

Game globalization

Both the US and China are pushing for new syntheses of connectivity and protectionism. This challenges other powers to do the same: the EU developed an investment screening-instrument on the one hand, to lay a halt to unwanted Chinese investments, yet is pushing for free trade with democratic Asian countries such as Japan. What will this in the long term mean for Europe's openness?

? Will Europe be able to finally broker a ground-breaking trade deal with India, like it has done with Japan?

Combine private and public sector strategies

China and the US, as well as Russia and Iran, have a strong track records of leveraging public and private innovation for military purposes. Is the EU willing and indeed able to merge these interests?

? Will European countries share resources to invest on a large scale in European cyber warfare? Will corporates, academia and states be able to synthesize strategies?

Own the new networks of power

China and the US have brought a new geopolitical Catch-22 upon Europe and European leaders and commentators call for 'strategic autonomy' or 'strategic sovereignty'. This means Europe must be able to flex its geopolitical muscle independent for instance when it comes to its relations to Russia, Iran or Turkey. If it wants to, it must own the new networks of power that the fourth industrial revelation will bring forth, as well as raise capital to rival China's push for connectivity in Asia. The EU as it stands now, does not have the capacity to do this. How will it muster the political will and unity to be bale to this? And will this not conflict with its values of freedom of information and protection of privacy as an open society?

? Will European economies decide to leverage state power to create European champions in the technologies that will dominate networks of power and security for decades to come?

Chapter 6
Into the unknown: how to plan for security ánd freedom

In his book Enlightenment Now[80], Steven Pinker argues that the world is in fact in a much better state than most of us think. The root cause of this is that we base our views on what we see and read in media reports. These nearly always stress the negative incidents rather than explore how the real developments 'under the hood' take place. Pinker puts forth a case for optimism. Panic that society is headed for self-destruction is not only unhelpful and misguided, Pinker says; it is inaccurate, based on the facts.

Could this be valid for the subject of this paper as well? Media reports are full of dystopian views. China will become a privacy monster; Europe will completely lose its role in the geopolitical arena; cyber warfare will lead us into a digital doom scenario. Doom scenarios seem to be the norm in this domain.

In order to have a fundamental discussion about this, we feel that we should paint a utopian future, thereby giving counterweight to the prevailing doom scenarios. Not because we predict that these scenarios will happen but because it is the best way to guide us to the really fundamental questions.

Moreover, we see many signals that there is in fact room for optimism. Again, we put the original question of Popper central: How can the open society remain strong in the face of foes and its own fragility, without sacrificing, **instead leveraging** its openness?

As an answer to this question, the following news articles from the year 2030 were conjured.

80 Steven Pinker – Enlightenment Now

BRAINPICKING THE DUTCH WAY: HOW CHINA FELL IN LOVE WITH THE TYPICAL DUTCH PUBLIC-PRIVATE COOPERATION IN DIGITAL TECHNOLOGY

Earlier this century, Chinese delegations came to learn how the Netherlands have brought agriculture to the next level using advanced technology. On the brink of a new decade, we now experience a completely new focal point of Chinese interest. This time, the Chinese would like to learn more about our triple Helix successes in AI.

Back in 2019, it didn't feel like a landmark decision when five Dutch companies – Ahold Delhaize, ING, KLM, NS and Philips – joined forces in 'Kickstart AI'. It was widely seen as a move to at least try to keep up with much faster developments in China and the US. Few could have foreseen that this coalition – and the accompanying investments – paved the way for a whole new model in how corporations work together with academic research and governments.

In ten years' time, 'Kickstart AI' has shown that the Dutch approach – based on a triple Helix model – simply works. It didn't take long for the Dutch universities to become a magnet for talented researchers in the AI domain. Some years later, international investors were eager to jump on the bandwagon. The success of the model now has Chinese policy makers wonder if they need to alter their strategy. For years, they followed a protectionist path in developing AI. But sources close to the Dutch ambassador to the People's Republic of China, Thijs de Vries, told us that highly placed officials are now eager to learn more about the ingredients of this Dutch approach based on public-private partnerships.

Rumor has it that the Chinese are divided about their strategy for the next seven years.One anonymous official was quoted to envy the unfolding successes of these partnerships.

PRESSURE MOUNTS ON US AS PNT 2 PROVES SUCCESS OF GLOBAL COLLABORATION

Officials from the European Union, China, Russia, India and Japan gathered in Brussels yesterday to celebrate the success of their joint global efforts in positioning, navigation and timing (PNT2) satellites. US president Hoover reclined to comment and looks determined to stick to his isolationist approach.

October last year, president Stephen Hoover reiterated his message again: “We have no intentions of becoming reliant on China for our strategic military and domestic objectives.” At least, this proves his consistent communication on this topic. But is an unsettling consistency, as prominent White House advisors have pointed out that the recently launched PNT2 system proves not only to be very successful but also to reach the next level in security.

The system has far reaching implications in several domains, including a significant increase in positioning and timing accuracy as well as on the geopolitical relationship with the United States. Although initially the United States was invited to join their GPS to the EU’s Galileo,

Chinese BeiDou, Russian GLONASS, India’s NavIC and Japan’s QZSS, the United States has consistently refused to collaborate. The unique cooperation created skin in the game from all members to keep the common objective in mind.

Even reports from White House researchers claim that the technical setup of the joint positioning system is designed to make it impossible for any one member of the collaboration to interfere with the integrity or availability of the system. A leaked memo confirms the difficult position that the US now have as a consequence of what is widely seen as another personal fight of ‘Stubborn Stephen’. From the memo: “US organizations will likely fall behind if we don’t find a workable solution to collaborate on and adopt innovations coming from abroad.”

AL WARFARE CONVENTION PASSES AS EUROPE STEPS UP TO THE PLATE AS THE NEW SUPERPOWER OF CONSENSUS

After years of escalations in AI-warfare between China and the US, and virtually no prospect of negotiating a truce, a historic diplomatic breakthrough was brokered by all 191 other countries in the world: the first global set of rules on the Future of Warfare.

In what is already being called the diplomatic Man-on-the-Moon-moment of the 21st century, a breath-taking 191 countries – all countries in the world except for the US and the PRC – have come together in Djibouti to sign the first UN Convention on the Future of Warfare, a document laying out strict rules and limits on the use of Artificial Intelligence and robotics in various kinds of conflict. As Indian president Singh said at a press-conference: "in the midst of hegemonic struggles, we often forget that the majority of people around the world have a clear interest and a heart-felt belief not in dominance, but consensus. Today is the real start of a truly multi-polar world, in which no great-power is great enough to push for standards unilaterally."

Widely acknowledged by insiders as the architect of the convention, the European commissioner for geopolitics De Vries, refused to comment on his personal contribution to the process, but instead read out a statement on behalf of all signatories. "This is only the beginning. The community of the shared destiny of mankind has spoken. It must now tackle the elephant in the room. The US and the PRC must be persuaded to subject to the rule of the convention. To this end, all signatories will lay sanctions on trade with the US and China until all hostilities have stopped." A senior Japanese diplomat called De Vries "a modern day Grotius", referring to the Dutch philosopher-statesman who first formulated principles of the law of the sea.

The point isn't to downplay the grave threats to the new security nexus of our societies. As we have shown, these threats are real and ubiquitous. The point is to show that leadership is not only needed, but indeed very well possible, to help the open society find new ways to game the hegemonic, technological and socio-cultural shifts of its security.

During the development of this paper, we have been convinced time after time, that Dutch and European leaders can and should take a leap of faith: invest in understanding China and their motivations ; invest in solid risk management to understand the risks of the new technological domains ; and dare to pioneer and collaborate with China on these domains.

As Popper argued, the status quo always presents itself as a historical necessity. Yet, we see it changing under our noses. The game is on, but we are not playing. It is high time European and Dutch leaders get in.

Acknowledgements

The research for this paper was conducted by Clingendael Institute and KPMG Advisory N.V. on their own initiative and for their own account. Many have contributed and helped shape this paper. We especially appreciate the insights, discussions and reflections of the experts and executives whom we have interviewed:

Frans Blom, Paul Dijcks, David Ferbrache, Peter Frankopan, Mark Greeven, Tom van der Heijden, Jaap de Hoop Scheffer, Lars Jacobs, Johan Kerst, Rem Korteweg, Frans-Paul van der Putten, Haroon Sheikh, Monika Sie Dhian Ho, Frank van Sprang, Koos Wolters and The Netherlands General Intelligence and Security Service.

About the authors

The authors, who work for Clingendael Institute and KPMG Advisory N.V., would like to thank all internal and external reviewers for their valuable contributions. They welcome you for a discussion on the conclusions from this report. You can contact the authors by email:

Ties Dams
Research Fellow
at Clingendael Institute
E: tdams@clingendael.org

Ruud Verbij
Manager Cyber Security
at KPMG Advisory N.V.
E: verbij.ruud@kpmg.nl

The authors would also like to thank Nart Wielaard and Marnix Bel for their support in the development of this paper.

Responsibility

Clingendael Institute and KPMG Advisory N.V. would like to make a constructive contribution to discussions about important social issues. The conclusions in this report are our own and not those of the reviewers or interviewees who have collaborated on this paper.

Organization:

TRANSFORMATION
FORUMS

Professor JH Bavincklaan 7-9
1183 AT Amstelveen
info@transformationforums.com
www.transformationforums.com

T +3120-299 6598