



GLOBSEC

Megatrends

2018





CONTENT

(Trend 1) Central and Eastern Europe is at its most geopolitically vulnerable since 1989	04
(Trend 2) The theoretical model of flexible integration is becoming reality	09
(Trend 3) More and more countries are losing faith in multilateralism	12
(Trend 4) The West is increasingly challenged by revisionist powers and ideological adversaries	18
(Trend 5) Global security relations are increasingly confrontational	22
(Trend 6) Ungoverned cyber space becomes an alluring setting for global conflict	26
(Trend 7) Technologies are increasingly weaponised to achieve political goals	30

Dear Reader,

A journalist once asked then British Prime Minister Harold Macmillan what is most likely to blow governments off course. “Events, my dear boy, events” was Macmillan’s alleged response. Assuming there is some truth in this statement, one can add that events, at least political ones, rarely drop from the sky as meteorites, strike as flashes of lightnings or come down as manna from Heaven. They occur in the context of wider or longer trends, having their origins somewhere and leaving traces as they pass. We are often guilty of ignoring the wider picture as we try to capture the significance of moments and disjointed facts. If the events are mice scurrying around in the bushes, the trends are big elephants, so big that we only see and touch their leg or snout without grasping the full scale of the giant.

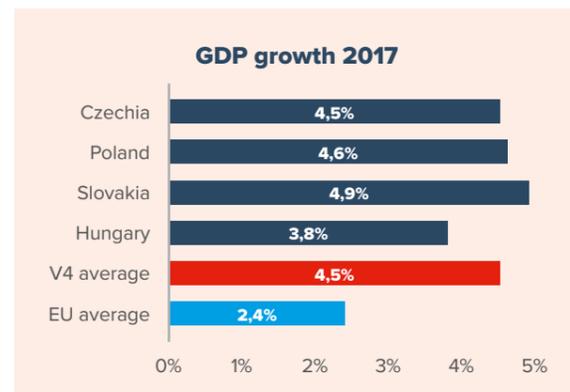
Trends are capable of doing more than turning governments off course, like the in case of one-off events. They can influence or decide the fate of societies and countries, determine their vital interests, choices or dilemmas. That is why staff at the GLOBSEC Policy Institute decided to conduct a thought experiment and – on the basis of year-round research activities at GLOBSEC (rather than pure conjecture) - try to identify seven major megatrends we believe to be the most important determinants of future of the West in general and Central Europe in particular. It would be a rather hopeless task if the list had an ambition to be exhaustive or if the phenomena we are writing about were to be properly explained or described. Faithful to the Shakspearian motto ‘brevity is the soul of wit’ we offer seven simple statements, risking the wrath of readers who are only satisfied with full argumentation and rigid methodology. They are:

- 1. Central and Eastern Europe (CEE) is at its most geopolitically vulnerable since 1989**
- 2. The theoretical model of flexible integration is becoming reality**
- 3. More and more countries are losing faith in multilateralism**
- 4. The West is increasingly challenged by revisionist powers and ideological adversaries**
- 5. Global security relations are increasingly confrontational**
- 6. Ungoverned cyber space becomes an alluring setting for global conflict**
- 7. Technologies are increasingly weaponised to achieve political goals**

As GLOBSEC Bratislava Forum 2018 draws nearer, we would like to play the role of provocateur and invite participants to a rather strategic and bird’s-eye view type of discussion. Each year, the GLOBSEC crowd (several thousands of us) gathers over three days to take part in dozens of events and sessions, with topics spanning technology, innovation through trade to security and defence, and beyond. It is easy to get drowned in detail while savouring the richness of debate at Central Europe’s leading forum on international issues. However, if you are ready and willing to take up our challenge, please spare a thought about your choice of megatrends and accept the invitation from GLOBSEC Policy Institute experts to debate these issues together during and after this year’s Forum. ●

(TREND 1) CENTRAL AND EASTERN EUROPE IS AT ITS MOST GEOPOLITICALLY VULNERABLE SINCE 1989

The Central and Eastern Europe of 2018 is flourishing much more than it ever has in the memory of its residents. Since 1989, the region has achieved remarkable progress. Prosperity is rising. Economically and politically, the countries are increasingly integrated within Western European structures. With accession to the EU came the opportunity to participate in the internal market, to have the unprecedented freedom to travel and work in the European Economic Area, and to receive much-needed flows of EU funds for rebuilding infrastructure or public investments. Today, Central Europeans are richer, happier, live longer and in a cleaner environment, and have better access to public services.



Source: European Commission 2018

Yet societies are far from satisfied. Freedoms in the single market, better quality of life, and peace are often taken for granted, especially by the younger generations. Furthermore, there are still unresolved issues that serve as sources of discontent. When their countries joined the EU, few people realized that it would take decades for some (e.g. Slovakia) to reach the development level of Germany, hence

the disappointment with the slower than expected rate of economic convergence. Central and Eastern Europeans often feel they are not accepted as equals on the European stage. For instance, Bulgaria's and Romania's aspirations to join Schengen have been trimmed. Croatia's, Bulgaria's and Romania's applications for the Exchange Rate Mechanism II were brushed aside. Additionally, much-needed EU cohesion funds are likely to shrink.¹

Bratislava, Warsaw, Zagreb and Sofia's bids for the relocation of the European Medicines Agency were unsuccessful. In fact, out of 45 EU agencies across Europe only 4 are in CEE.

In most international indexes for development CEE still ranks distinctly worse than Western Europe – from corruption and business conditions to education and quality of governance. It takes time to remedy these shortcomings, given the shorter institutional memory, less established Western political culture, and the remnants of post-communist mentality in the region. The economy is likewise poorly-adjusted to weather the storms of the digital post-industrial future. It is still subsidiary in the production chain to Western economies, dependent on foreign investments, and increasingly haunted by low productivity.

From inside or outside, the region looks vulnerable. External conditions are worsening for Central Europe. In contrast to the time when the region was joining, the EU itself is in flux. Once again, it is searching to re-define or reinvigorate its identity and purpose.

Comparative ranking in development indexes			
	Corruption Index 2017	Ease of Doing Business Index 2017	Human Development Index 2016
Denmark	2	3	5
Germany	12	20	4
Poland	36	27	28
Czechia	42	30	36
Slovakia	54	39	40
Hungary	66	48	43

Source: Transparency International 2017, World Bank 2017, UNDP 2017

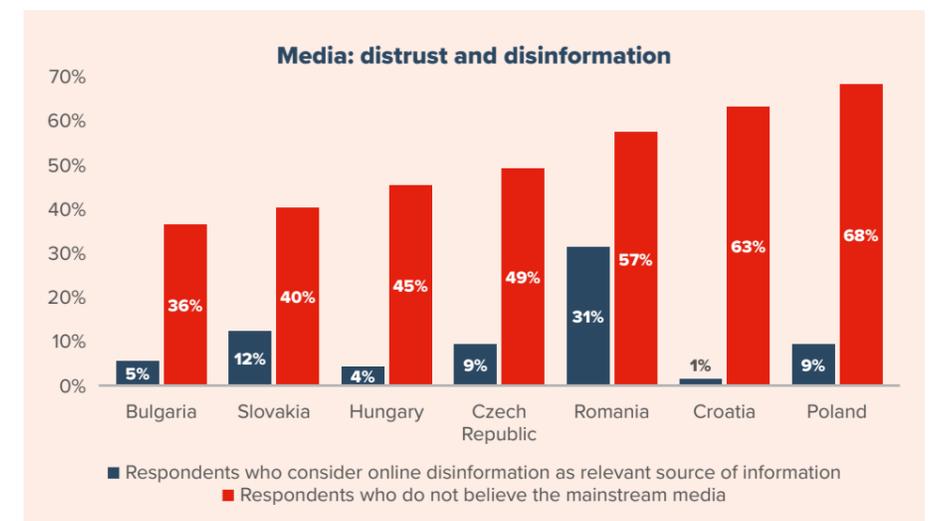
The UK is leaving the Union and the negotiation process has been slow and painful. It is, however, the period after Brexit that will serve as the true stress-test for the Union. Politically, new internal alliances will be formed. The UK has been a good partner for Central and Eastern European countries in policy areas such as labour and social policy. Economically, the UK market and its financial services will be more expensive and less available. Socially, the limitation of free travel and work in the UK might change the composition of some CEE regions – fewer (younger) people will leave and some of those who left earlier may come back.

Brexit aside, the Union is still reeling from the blow of the 2008 crisis. Discussions on convergence and budgets stumble on the overbearing logic of juste retour. Proliferating economic nationalism and ideological divisions transcend the topics of migration, rule of law and foreign policy.

Some European reforms are simply overdue, including stabilising the euro-zone and completing the single market and Schengen. The window of opportunity is quickly closing for endeavours to re-shape the EU to be more attractive to its citizens, more economically and financially stable and more democratic.

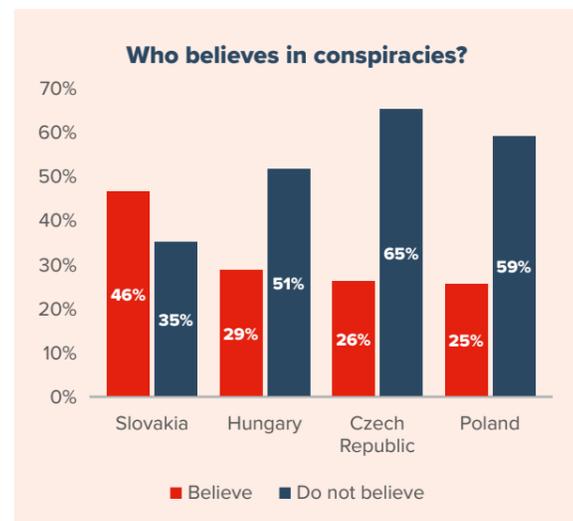
The upbeat character of 2017 with grand speeches from EC President Jean-Claude Juncker and French President Macron has been already toned down.

It's not just Europe. The West, in general, has lost much of its magnetism in relation to the rest of the world. Multilateralism is in crisis, with international organisations unable to facilitate dialogue and international actors unwilling to commit. In the meantime, modern society is evolving and the long-term influence of new technologies on democracy and media will have consequences that are hard to foresee today. New technologies have already shifted discourse into the social media realm, enabling demands for direct and swift communication with the public. At the same time, the new tech-based communication paradigm has also been transformed into a theatre of information war.



Source: GLOBSEC Trends, 2017

False information is mushrooming in Central Europe, often purposefully planted and disseminated to inflict damage on the still young democracies. Both external and domestic actors are attempting to mould the geopolitical orientation of CEE countries to their liking, and this liking is often not on the side of the EU and NATO.



Source: GLOBSEC, 2018

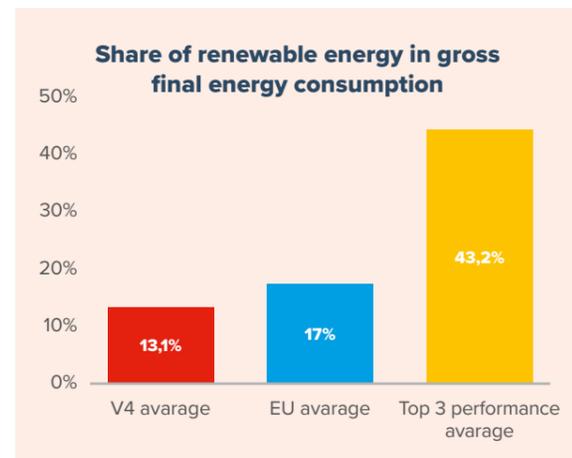
According to GLOBSEC Trends 2017,² 10 million people in CEE use disinformation websites and trust them as a relevant source of information. Fewer people rely on or trust traditional media, with its principle of fact-checking, while more people receive information primarily from social media.

Russia is frequently identified as the powerful force behind coordinated misinformation implants. The information space is, however, not the only arena for geopolitical wrestling. Confrontation between Russia and the West is escalating. Poisoning with a military-grade nerve agent in the UK or the civil war in Syria with gross human rights violations all have repercussions for the CEE region.

Closer to home, the conflict in neighbouring Ukraine and military build-up in the Baltic region and Crimea hardly give any grounds for the Baltic countries and Poland in particular to consider their proximity to Russia as a stabilising force. Russia has now developed special zones of defence capabilities, following the “anti-access and area denial” concept. These zones are now part of Moscow’s efforts to turn its armed forces

into a more-compact, mobile, technologically-advanced military that’s capable of projecting force in an efficient manner across a wide spectrum of potential (conflict) scenarios.”³

In addition, the longstanding and almost total dependence on Russia’s gas supplies and wide network of business links has not diminished. The completion of Nord Stream II will endanger the region’s access to necessary supplies. Renewable energy infrastructure and capacity is almost non-existent in comparison to traditional energy sources. If Central and Eastern Europe is not able to diversify and, in the meantime, push for safeguards and guaranteed supplies, then the region’s vulnerability will only increase year by year.



Source: Eurostat 2017

It is not just Russia expressing strong interest in the region. China is also seeking to gain influence through (often aggressive) economic expansion. Beijing’s long-term strategy for Europe is relatively transparent. The more China invests in the CEE region, especially in areas where more funds are necessary, the stronger the pro-Chinese lobby in Brussels will be. Tough decisions will be on the EU table, covering trade imbalances, fair competition laws, strategic investment screening (as suggested by France), human rights and the overall EU policy towards China. As China sees it, CEE countries might prove useful allies in these debates.

It is not a coincidence that five years ago China unveiled a massive ‘infrastructural’ project – the “one road, one belt” initiative. Within the initiative, the 16+1 framework was structured for China to enter

Central Europe and the Western Balkans.⁴ Most 16+1 countries, with certain reservations, allowed China to set up activities on their soil. These range from Confucius Centres and tourism agencies to offers of large financial loans for infrastructure boosts and high-skill industries. While EU competitiveness regulations have kept large scale projects at bay in CEE countries, the Western Balkans have taken up the opportunity.^{5,6} Direct investment is growing although the impact is not that large at €7.5 billion, up from €3 billion in 2012.⁷



Source: CSIS, Financial Times 2017

While new powers are paying more attention to Europe, US President Trump’s “America first” domestic and foreign policy is a sobering reality check, particularly for CEE. Global trade wars are one step away and, if not averted, will leave no winners in the end. With “America first”, the world leadership position is vacated. It is a scenario that is particularly felt by Europeans, given that US support for preserving the EU as a strategic objective of its foreign policy is no longer present.⁸

Not all is quiet on the Southern front either. Uncertainty regarding the prospects of the Western Balkans joining the EU is fuelling nationalistic and anti-European sentiments across societies which are, in turn, skilfully perpetuated by local politicians. Moreover, as the EU withdrew from the region, others filled the void. Beyond China’s “one road, one belt” initiative,⁹ Saudi Arabia has sponsored schools and mosques,¹⁰ Turkey has rapidly increased regional trade,¹¹ and Russia has made its presence felt within business and politics.¹²

With stabilising actors out and destabilising actors in, continued interstate tensions, territorial claims and ethnic strains will hinder closer regional

cooperation. A propitious environment is in place for violent extremism and radicalisation, the levels of which are increasing particularly rapidly in Bosnia and Herzegovina¹³, Kosovo¹⁴ and Macedonia.¹⁵ In this context, the proliferation of extremist groups on the doorstep of the CEE region brings serious security threats. In addition, the “Balkan routes” used for illegal flows such as human trafficking, weapons, narcotics and counterfeit goods simply sprout onwards through CEE and into Western Europe.

All these phenomena touch the West in general but are particularly rattling CEE countries. Still less economically developed and politically and socially stable, the region is more affected by multiple challenges and challengers. The overall crisis of liberal democracy is especially acute in CEE. According to GLOBSEC Trends 2017, 37% of Bulgarians see autocracy as the best political system for their country, compared to 42% who prefer liberal democracy.¹⁶ Sympathies for Vladimir Putin are abundant in CEE countries with 70% of Bulgarians and approximately 40% in Romania, Croatia, Hungary and Slovakia supporting the Russian president’s policies. According to a Gallup International survey, citizens of some CEE countries, such as Bulgaria and Slovenia, would still prefer to turn to Russia if a major security crisis erupts.¹⁷

Euroscepticism is similarly on the rise in Central Europe. Societies and political elites are increasingly concentrating on the differences, rather than similarities, between the region and its Western European counterparts. While in the past there was a broad attempt to catch-up with the West and showcase a common understanding of the world, today’s CEE is seeking a divergent (own) identity. This collision course between the East and the West is aided by opposing attitudes towards sexual minorities, ethnic diversity, capital punishment, religion, and functioning of democratic institutions, to name a few, where often the positions of the Western EU are more liberal and open.

Euroscepticism is also becoming institutionalized in some parts of the region. Poland and Hungary have governments who perceive the EU as deeply flawed both in terms of founding principles and institutional set-up. Such an outlook then aids the political misuse of European issues for domestic gains.

It has become a widely spread practice to blame “Brussels” for domestic policy failures, sometimes building a dangerous rhetoric with clear nationalist agendas. Thus, new policies that are being enacted are defended in the domestic realm, even if they contradict EU regulations and values (e.g. judiciary laws in Poland, the ‘foreign agent’ law in Hungary).

Conclusions and recommendations

All this means that Central Europe is less embedded in the EU just as it needs it most to stave off hostile actions from outside. Support for NATO in the region is stable but the role of the alliance is confined to the provision of military security. The nature of the challenges ahead of the CEE is much more diverse. This brings us to recommend the following:

- ▶ The returning East-West divide in the EU needs to be reversed at all costs – through actions of decision makers on both sides and proper debate with citizens.
- ▶ European unity should not be taken for granted. It needs to be built and sustained through active measures. There is a case for strong and impartial EU institutions as these can guarantee an even-playing field between Member States.
- ▶ Solutions to disputes that have grown out of proportion need to be found quickly. For example, the disagreements over how to manage migration are much bigger than the issue’s practical salience for the region.
- ▶ The EU should seize the opportunity to re-unite by addressing common challenges - information warfare, defence, and internal security.

Our work illustrates GLOBSEC’s commitment to enhancing security, prosperity and sustainability in CEE and Europe. The GLOBSEC Intelligence Reform Initiative calls for provides a roadmap for a Centre of Excellence, whereas our NATO Adaptation Initiative proposes 10 key elements for a new NATO strategy. Simultaneously our Strategic Communication projects monitor and counter disinformation implants in Central Europe, while the future Vision for Europe taskforce will outline an action plan for reversing the East-West divide. ●



(TREND 2) THE THEORETICAL MODEL OF FLEXIBLE INTEGRATION IS BECOMING REALITY

Once a theoretical concept, flexible integration is becoming a ‘normal’ feature of mainstream European integration discourse.

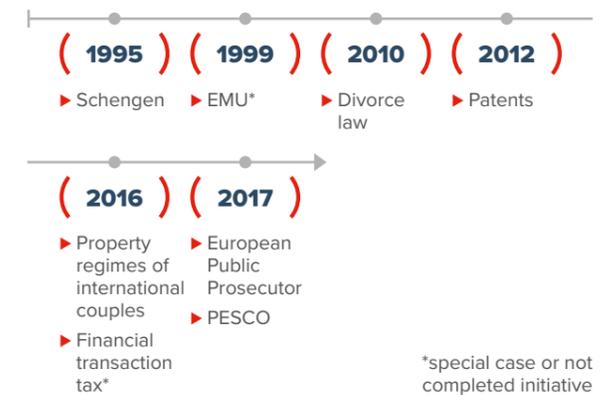
For a long time, scholars have been debating the possibility of the EU to moving forward on more flexible terms.¹⁸ Two-speed Europe, Europe à la carte, variable geometry, differentiation and concentric circles are all concepts explaining in theory how Europe can be shaped not through a single institutional order but alternative ways to manage divisions and disagreements.

Europe à la carte
Two-speed Europe
Multispeed
Two tiers
Variable geometry
Differentiation
Abgestufte integration
Concentric circles
Exclusion of the uncooperative
Core community

The concept of flexibility in European integration can be found in several Treaties: The Single European Act (1986), the Treaty on European Union (1997) and the Lisbon Treaty (2007). Yet, until the UK’s decision to leave the Union, the idea itself was either feared, as it might lead to disintegration, or snubbed as politically inappropriate. Today, it is no longer a taboo to seek other alternatives to unified integration. Rather, member states and EU institutions are eager to exploit differentiation.¹⁹

Prescient analysts long predicted that the next generation EU would combine three (dis)integration developments: accelerated integration for some, disintegration for others and greater flexibility in commitments to European policies and institutions for all members.²⁰ Their observations are starting to be fulfilled. France and Germany are devising a plan for 'ever closer EMU' and 'enhanced cooperation' initiatives are on the rise with the Permanent Structured Cooperation (PESCO) and the European Public Prosecutor's Office (EPPO) in more developed stages.

The initial shock from the decision of the UK to leave provided impetus for the EU to carefully assess its future. One of the reasons behind the British discontent with the EU, at least in the minds of voters, has been the perceived lack of flexibility and inability to fully accommodate the preferences of the British. And so, to avoid other exits, the European Commission accelerated its careful but vocal evaluation of the possible future scenarios for the EU.²¹



*special case or not completed initiative

Meanwhile, the eurozone has transformed into a distinct formation, a new union inside the Union. The eurozone countries are on their way to further solidifying their influence in the EU. This June, France and Germany will present a concrete framework on how the eurozone can be more stable, predictable and resilient as new economic crises approach.^{22,23}

While there is an ideological divergence among Eurogroup members about financial responsibility and solidarity, all agree that further integration is a must. The proposed reforms might be expressed by completing the banking union with joint European deposit insurance for financial institutions, a capital markets union, possibly agreeing on unemployment insurance and transforming the stabilisation fund into a European Monetary Fund. In future there even might be a eurozone budget, finance minister, Parliament and Treasury.

Naturally, those EU members that are also in the eurozone will enjoy more leverage over non-members. This shift in power relations, therefore, will cascade onto matters that are of importance not only to the eurozone but also the whole Union.

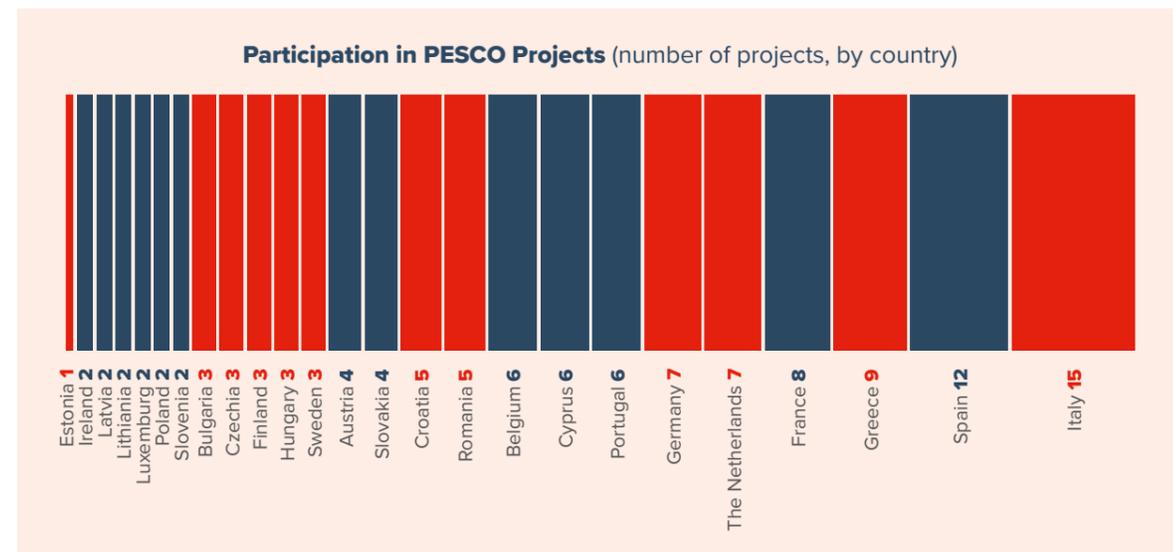
Besides covering the rather conventional areas of monetary and economic integration, acceptance of the 'Union of Unions' logic has emboldened integration moves in areas that the EU previously shunned.

As security affairs move up in the ranks of priorities and concerns for European citizens, the EU political elites seek to address public demand for political action on defence cooperation through the concept of Permanent Structured Cooperation (PESCO). Initially, PESCO was to be an exclusive platform for ambitious European defence stakeholders. Today, however, a more inclusive approach has prevailed—with 25 out of 28 EU members signing up to the initiative (with the notable exceptions of the UK, Malta and Denmark).²⁴

Interestingly, in its current form, PESCO provides a substantial amount of manoeuvring space for member states to articulate the level of ambition they seek to associate with PESCO. As a direct result of this setting, Italy participates in 15 projects (from the overall 17), Spain in 12, while other European defence actors, for example Poland, only in a handful.²⁵ This diversity of engagement represents the core of the flexible integration principle, within which member states not only choose in which policy areas they seek greater and deeper policy alignment, but also decide on what segments of the chosen policy areas are worth coordinating.²⁶ It is, however, already noticeable that Western European members' level of commitment to different projects is higher than their CEE counterparts.²⁷

Conclusions and recommendations

- ▶ Flexible integration can be a way to alleviate concerns about deeper integration and an opportunity to move forward in different policy areas. The mechanism, however, needs to have clearly set non-exclusive conditions and to be pursued when an added value to the agility of the whole Union is present. East-West or North-South divides should be avoided at all cost.
- ▶ While non-eurozone members should consider how further integration will affect their future standing in the EU, the Eurogroup should move forward with making long overdue reforms. But they should not be closing the door to willing and able candidates. ●



Source: European Commission 2017

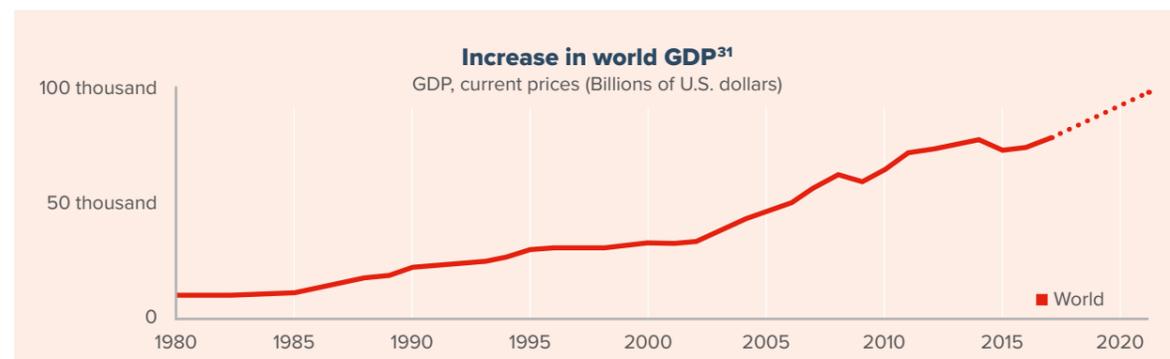
(TREND 3) MORE AND MORE COUNTRIES ARE LOSING FAITH IN MULTILATERALISM

Multilateralism experienced its 'golden age' in the second half of the 20th century. The framework of international organisations covered many areas such as security, trade, banking, culture, climate change and many more.²⁸ The United Nations (UN), NATO, World Trade Organization (WTO), and others shaped the backbone of a rules-based global order.

The achievements of the global governance system are immense. First and foremost, it contributed to building an environment free of global military conflict. For example, it discouraged countries like Germany, Japan, Saudi Arabia and South Korea from acquiring nuclear powers.²⁹ The World Trade Organization has managed to increasingly integrate national economies and tempered unilateral approaches to international trade.³⁰ Under the WTO, international cooperation among 164 countries representing 98% of the global economy has resulted in a significant liberalisation of world trade, especially in goods, which led to substantial economic benefits and contributed to an increase in global GDP. Over the past two decades, global GDP grew by 240%, from \$30.8 trillion in 1995 to \$75.8 trillion in 2016.

Moreover, the Montreal Protocol signed under the UN framework in 1987 led to a substantial decrease in the emission of ozone-depleting substances and is one of the most successful examples of international environmental cooperation to date. The creation of the International Criminal Court (ICC) in 2002, an institution to ensure that crimes against humanity and mass atrocities do not occur with impunity, is another success story of multilateralism.

Some of the recent examples of multilateralism benefits include the OECD/ G20 Base Erosion and Profit Shifting (BEPS) package that refers to tax avoidance strategies that exploit gaps in tax rules to artificially shift profits to low or no-tax locations. Currently, 113 countries and legislations have joined the initiative.³² Last, but not least, the Paris Climate Agreement signed in 2016 is a major success for the United Nations and intergovernmental cooperation and is the first major multilateral deal of the twenty-first century. It sets out a global action plan to put the world on track to avoid dangerous climate change and pursue efforts to limit any temperature increase.



©IMF, 2007, Source: World Economic Outlook (October 2017)

Despite their achievements, both multilateral institutions and the liberal international order in which they are rooted are today being questioned. Successive shocks — the global financial crisis, the eurozone crisis, and the migrant influx into Europe in 2015 — have set the stage for political backlash that now besets global governance.³³ It is observed that smaller or poorer states are growing increasingly discontented with what they see as the institutionalization of global inequality and discrimination while powerful states are increasingly unwilling to be constrained by multilateral norms.³⁴

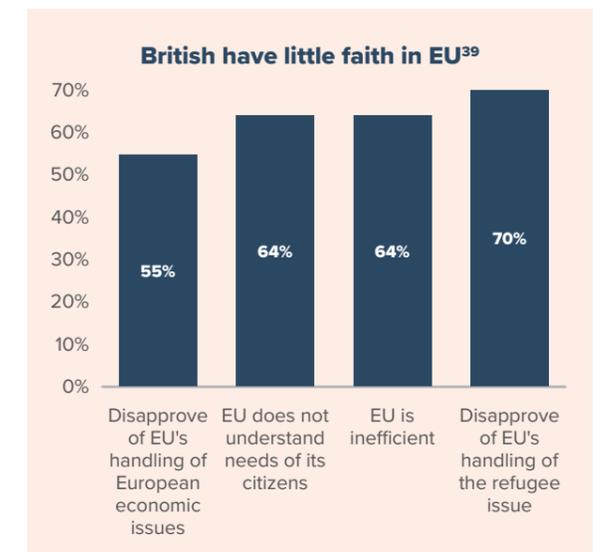
The main reasons for losing faith in multilateralism are increased polarisation and fragmentation in world politics, as well as a lack of effectiveness and representation in many multilateral organisations.³⁵ Many believe that the structure of some international organisations has outlived its usefulness, as is the case of the UN Security Council. Consequently, the BRICS (Brazil, Russia, India, China and South Africa) keep pushing to renegotiate existing global governance arrangements and enhance their role in them.

Another argument points to the fact that many organisations are failing to deliver on their declared goals, which perhaps were too ambitious to begin with. For example, the World Bank has been unsuccessful in eradicating global poverty, and the UN in promoting effective regional peace and stability. Additionally, the WTO has failed to conclude the 2001 Doha Development Round of trade negotiations and is unable to address new trade issues such as e-commerce or protection of intellectual property that have arisen since its creation in 1995 and led to trade imbalances. According to some observers, the recent trade war between the US and China occurred because the WTO and global trade rules are ill-equipped to referee China's rise.³⁶ To sum up, many believe that today's international organisations are not capable of solving today's problems.

The phenomenon of losing faith in multilateralism has also been attributed to the widening gap between public and international institutions. People feel that many deals are done behind closed doors. In fact, it was partly a lack of awareness that caused the mass protests that brought down

the Anti-Counterfeiting Trade Agreement (ACTA) in 2011. The EU was also accused of secret deals while negotiating the Comprehensive Economic and Trade Agreement (CETA) with Canada and the Transatlantic Trade and Investment Partnership (TTIP) with the US. A very low proportion of respondents felt sufficiently well-informed about the process.³⁸ It is also worth mentioning opposition in countries like Greece and Spain to austerity measures implemented by the so-called Troika — the International Monetary Fund, the European Central Bank and the European Commission. In return for getting access to additional financial resources the countries were forced to accept harsh fiscal tightening and social deregulation, which caused discontent among the people.

The perception of international organisations as being inefficient and representing the interest of cosmopolitan elites partly explain why the majority of the UK electorate voted for Brexit. The "Leave" campaign, which won by a slim 52-48% margin, focused precisely on the issue of restoring national sovereignty.



Source: Pew Research Centre 2016

Finally, some of the causes of this crisis are related to the decline of American power and the fact that the old liberal international order was designed and built by the West. Brazil, China, India, and other emerging powers have a different set of cultural, political, and economic experiences, and see the world through their anti-Western grievances.⁴⁰

Global rules are being rewritten on the US watch

The United States, the most powerful state in the post-war world and driving force behind liberal multilateral arrangements, is today withdrawing from the world. Donald Trump's Presidential campaign was explicitly nationalist in tone and content.⁴¹ From the outset, the now US President expressed preference for bilateralism over multilateralism in trade and questioned several existing multilateral arrangements in climate, development, humanitarian, trade and security policy.

In fact, President Trump called NATO obsolete, criticised the European Union's shared policies – like climate change, free trade and defence – and left the Paris Climate Accord. Moreover, the US is at the centre of the rewriting of global trade rules. The current US administration abandoned TTIP, withdrew from the Trans-Pacific Partnership (TPP) (that now is considering joining back) has embarked on a never seen before renegotiation of the North American Free Trade Agreement (NAFTA) and imposed broad tariff on imports on steel (25%) and on all aluminium (10%).⁴² The Trans-Pacific Partnership was important for multilateral order because it was regarded as a tool for expanding the NAFTA model to Asian and Latin American countries (12 countries).⁴³ In the case of Asia, a widening of NAFTA arrangements was expected to help promote the bloc's common trade agenda worldwide by creating a universal set of rules and market access commitments. Domestically, it was decided to reboot NAFTA, an agreement that has long been a populist punchbag. After the US withdrew from the agreement in January 2017 the other 11 members of TPP renamed the deal as the Comprehensive and Progressive Agreement for TPP (CPTPP) and are now in the process of ratification.⁴⁴ Mexico became the first country to ratify the CPTPP on 26 April 2018.

While it has long been clear that NAFTA needs to be reformed, never has the agreement been renegotiated in such depth. Optimists argue that the recent crisis will bring Mexico and Canada closer together, while realists warn the deal does not make any sense without US involvement. Indeed, given the high-level disagreements over

the deal (foremost about trade in vehicles and their parts),⁴⁵ progress towards sealing it this year is, in effect, unrealistic. However, the new deal will be signed sooner rather than later'as the stakes for the US are too high just to abandon it (as happened with TTIP or TTP).

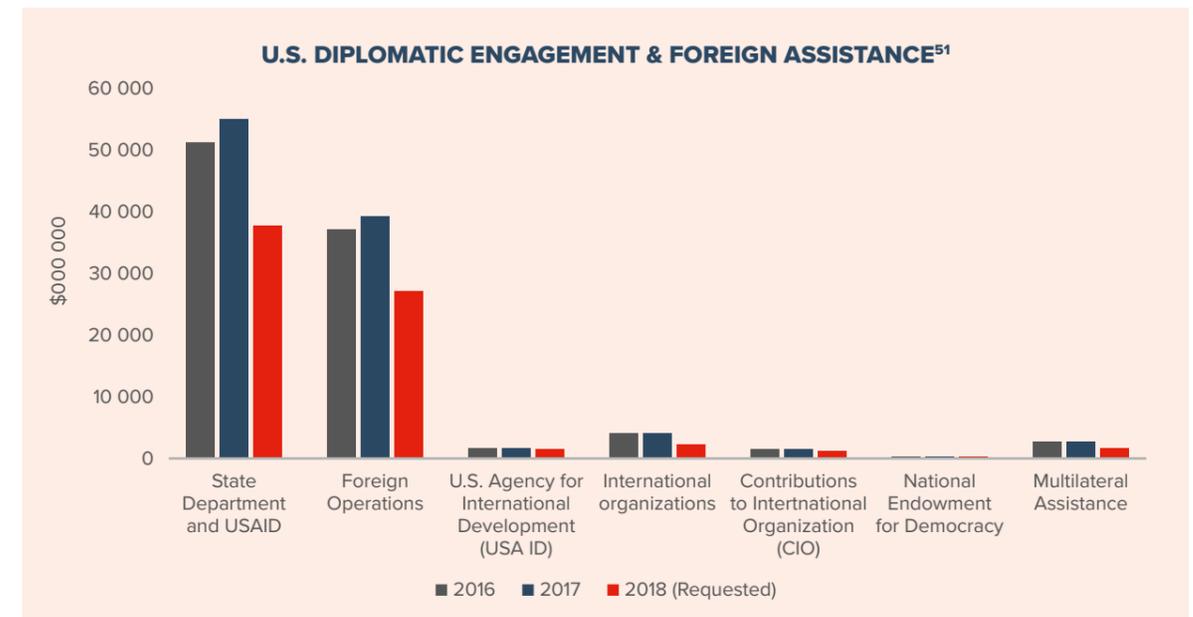
Global trade in 2018 will be overshadowed by the US decision to impose broad tariff on imports on steel (25%) and on all aluminium (10%), foremost from China and Japan (at the time of writing the EU, Canada and Mexico are excluded). The Financial Times estimates that the world's two largest economies are currently on the brink of a \$100bn trade war because China has already presented its retaliatory list of more than 100 US exports including soybeans, aircraft and cars.⁴⁶

The current dispute threatens the role of the WTO. The invocation of the national security exception (a reason to introduce protectionist measures by the US) in this case has implications that go beyond narrow sectoral effects and it represents a challenge to the world trading system.⁴⁸ At the end of the day, the WTO will have to rule in favour of one of the US or China. If the ruling is in favour of the import tariffs, it may encourage the use of national security concerns as a pretext for trade protectionism from other countries. If China wins the case, the Economist foresees that the US will not drop tariffs but undermine the role of the WTO instead.⁴⁹

Lastly, the US has recently decreased its financial commitments to multilateral organization. Not only the State Department budget was cut by 32% but also its contribution to international organisations and multilateral assistance were both decreased by 43%. The new US administration also withdrew all funding for anything to do with climate change such as the Clean Technology Fund and the Strategic Climate Fund.⁵⁰ Other entities that did not get any funding in 2018 were the International Bank for Reconstruction and Development, Asian Development Fund, Inter-American Development Bank North American Development Bank and the Global Agriculture and Food Security Program. Moreover, the funding of programmes such as the Asia Foundation and East-West Centre was also cut. It is also worth mentioning that the budget of the

National Endowment for Democracy, which since its creation in 1983, has spearheaded American efforts to foster democracy throughout the world, was cut by 38%.

weaken the EU's diplomatic weight. However, Brexit can grant the EU more internal political space. That is because the UK, despite being one of the most constructive builders of a multilateral liberal order,



Source: US State Department 2018

The EU reinvigorates its multilateral agenda

Since the EU's creation, multilateralism has remained at the core of European identity and its engagement as a global actor. Both the 2003 European Security Strategy and the 2016 Global Strategy stress its importance and made its promotion part of the EU's strategic goals.⁵²

It is also worth mentioning that the EU and its member states were the world's largest aid donors in 2015 and the biggest combined donor to the UN. This amounts to 30% of the regular budget, 33% of the peacekeeping budget, and roughly 50% of all voluntary contributions to UN programmes and funds. In this sense, multilateralism is not only important for the EU, but the EU is also important for multilateralism.⁵³

However, the EU is by no means the perfect multilateral organisation. For instance, its internal market (or single market) remains a work in progress and there is increasing nationalism and protectionism in many member states. There is no doubt that the United Kingdom's (UK) departure will

was to some extent reluctant to enhance the EU's multilateral representation.

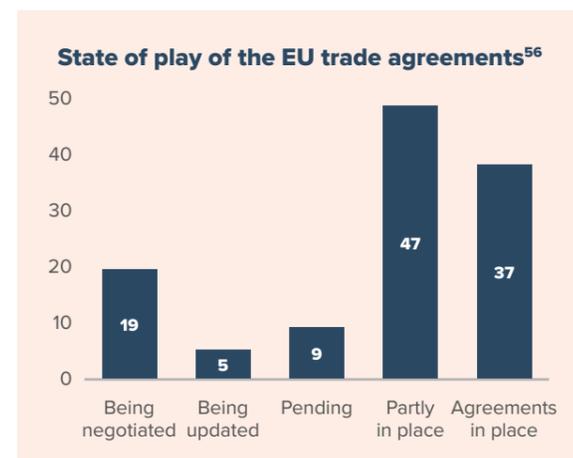
Today, the EU tries to show its commitment to multilateralism by forging new trade deals, showing neighbouring countries that it is still an interesting project and filling the void of the US leadership in areas like the Paris Climate Accord or upholding the nuclear agreement with Iran (the Joint Comprehensive Plan of Action).

The EU is doing its best to frame itself as the leading proponent of global free trade. This was also the case in the past when in 2013 it backed negotiations of the Transatlantic Trade and Investment Partnership (TTIP). Apart from creating jobs and fostering economic growth, the EU aimed to cement the transatlantic alliance and set mutual standards that the rest of the world would have to follow.⁵⁴

Last year, the block signed the Comprehensive Economic and Trade Agreement (CETA) with Canada, which has provisionally entered into force (it is now being ratified by member states' parliaments) and

concluded free trade talks with Japan. Brussels has also announced that is a “window of opportunity” for a deal with Mercosur (Argentina, Brazil, Paraguay and Uruguay). In fact, trade talks between the EU and Mercosur have never been so cordial and a deal will most probably be concluded sooner rather than later (possibly before the presidential elections in Brazil on 7 October 2018). Apart from South America, the EU is negotiating with countries such as Australia, New Zealand and India.

It is not risky to say that the EU might now be tempted to go for quick rather than ambitious deals to show the world that, contrary to the US, it still believes in the global governance model. EU member states have access to roughly 84 countries where trade agreements are either fully or partially in place.⁵⁵



The EU is also trying to show its neighbours that it is still a compelling project. Jean-Claude Juncker the president of the European Commission, in his 2017 State of the Union address underlined the importance of the Western Balkans joining the EU in the future. Consequently, in March 2018, the European Commission adopted 'a credible enlargement perspective for and enhanced EU engagement with the Western Balkans.⁵⁷ This includes a commitment to being seen as engaging actor for once politically unpopular enlargement policies.

While in the short term, we should not expect any country to join the EU, we could expect new members to join the EU in the medium term (2025).

Those could be most probably Montenegro and maybe Serbia, provided it normalizes relations with Kosovo as requested by the Chapter 35 of the accession negotiations.

Conclusions and recommendations

Despite EU efforts, the question remains if the deeper system of liberal internationalism at the core of today's international order still holds sway if the US is not in the game. It's safe to predict that in the short term, even without the US, the system will prevail. However, if the US does not regain trust in multilateral order, its future may not be so bright in the mid to long term.

With new powers and complex challenges emerging in different regions global decision making is relying ever more strongly on multilateralism. Challenges such as nuclear non-proliferation, climate change and promoting global trade cannot be tackled otherwise. That is why the US and EU need to work together to “reinvent multilateralism and to create a new 21st Century world order” as suggested by French President Emmanuel Macron in his recent speech in the US Congress.

To achieve this, policy makers and experts should:

- ▶ Build on the achievements of the global governance and consolidate the commitments to strengthen multilateralism.
- ▶ Recognise the weaknesses of multilateral institutions and be open for reforming organisations such as the UN or WTO.
- ▶ Aim for dialogue with emerging powers that are currently under-represented in global governance institutions.
- ▶ Bring multilateral institutions closer to the citizens and make sure that they understand the benefits of being part of them.
- ▶ Emphasise that the EU needs to be proactive in safeguarding multilateralism and look for new partners for multilateral cooperation while acknowledging and promoting the necessary reforms to the architecture of global governance.

- ▶ Bound by shared values, the EU and the US should keep working together to promote the shared values of freedom, democracy, and the rule of law worldwide, laying the foundations that create stable and prosperous partners around the globe. ●

(TREND 4) THE WEST IS INCREASINGLY CHALLENGED BY REVISIONIST POWERS AND IDEOLOGICAL ADVERSARIES

Since 1989 Europe has remained largely peaceful (with some exceptions of armed conflicts in the Balkans, Caucasus and Ukraine) as its eastern part democratised and most Central and Eastern European countries joined NATO, the EU, or both. This reality has not changed in 2018 and the West is not about to go through a devastating and prolonged military conflict.

Nonetheless, the world, and especially the NATO Allies and EU Member States, have witnessed a string of less explicit, seemingly low key challenges to their freedom and security. These emanate from “revisionist” states⁵⁸ which oppose the liberal world order. Other challengers are non-state in nature but can be, if needed, hired or inspired by states. These include organised criminals, who join forces with ISIS and other terrorists to smuggle narcotics into and via Europe,⁵⁹ and jihadists who, via their bombings, shooting and stabbings in the streets of European cities, have been waging war on the West for two decades.⁶⁰ Finally, there are paramilitary groups outside the control of states, whose members train in “revisionist” states. These include veterans from the Ukraine conflict.⁶¹

These forces are more interested in the slow and steady erosion of the West’s status rather than its complete downfall. Unlike events before 1989, or the regional conflicts of the past decade, these contributions come in different shapes and forms and constitute the most direct and lethal threats

to the Western world. Such a slow and deliberate strategy means that the enemy has to be attacked more often but with smaller thrusts.⁶² These will not spell the end of the West as we know it, and on their own will not constitute a strategic threat

to NATO Allies or EU Member States. Nonetheless, their repetitive character provides a powerful narrative in which the attacked, under-siege West is threatened, endangered or retreating.

The GLOBSEC NATO Adaptation Initiative Final Report neatly summarises the challenge facing the broader West. It emanates not only from the East (read: Russia) and from the broader South (read: terrorism and terror-related developments from the MENA region)⁶⁴ but also from within, such as terrorist attacks, targeted killings, and criminal acts taking place in the Transatlantic area. Both ISIS⁶⁵ and Russia⁶⁶ consider themselves at war with the West and as weaker challengers they will use such methods to harm their opponent.⁶⁷

To harm the West, challengers increasingly use Western inventions and capabilities against their targets. Examples are numerous.

By exploiting vulnerabilities in the Schengen system, ISIS was able to hide operatives amongst

the refugee-migrant masses traversing Europe in 2015. At the same time, the organisation utilised widely available and seemingly harmless technologies to direct terrorist plots in the West by “remote control”, literally texting, via encrypted apps, targeting instructions to attackers.⁶⁸

Nowadays, China is widely seen as a bigger threat to the U.S. or the West than Russia.⁶⁹ Beijing tries to turn Chinese nationals working at US universities into spies so that it can benefit from the illegal transfer of technologies developed at Western academic institutions.⁷⁰

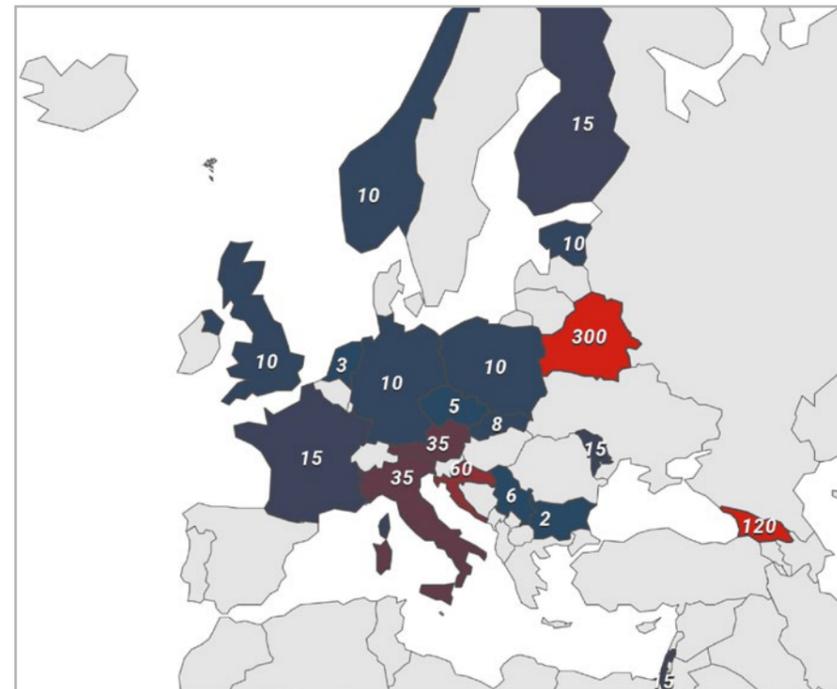
Utilising the free movement of capital, Russian-controlled banks and Kremlin-connected intermediaries based in the EU sponsor European political parties and projects with an anti-EU message.⁷¹ Moreover, free movement of persons allegedly enabled a team of Moscow-organised assassins to poison Sergei Skripal, a former Russian military intelligence officer, with the Novichok nerve agent.⁷² The same free movement of persons,

STATE OF TERRORISM											
											
	Austria	Belgium	Bulgaria	France	Germany	Greece	Italy	Ireland	Netherlands	Spain	United Kingdom
Official threat level	elevated	2 (out of 4)	3 - low (out of 3)	-	-	1 - low	2 (out of 3)	2 (out of 5)	4 - substantial (out of 5)	4 (out of 5)	4 - severe (out of 5)
Terrorism arrest 2015 (Jihadi arrest)	49 (48)	61 (60)	21 (21)	424 (377)	40 (21)	16 (Left-wing)	40 (40)	41 (Separatists)	20 (20)	187 (75)	134 (Not specified)
Terrorism arrest 2016 (Jihadi arrest)	34 (30)	65 (62)	5 (5)	456 (429)	35 (25)	15 (Left-wing)	38 (28)	16 (1) (Separatists)	45 (36)	120 (69)	149 (Not specified)
Foreign fighters	296 (51 attempted to leave)	589	1	2147	950	0	110	-	280	139	850
Killed foreign fighters	45	129	0	281	-	0	-	-	44	-	100
Returned foreign fighters	90	102	1	302	-	0	10	-	50	25	430
Convictions for terrorism in 2015	27	116	0	14	17	38	0	0	18	166	106
Convictions for terrorism in 2016	26	127	0	66	30	3	11	-	42	154	89
Victims killed in terrorism attacks 2015	0	32	0	147	1	1	0	-	0	0	1
Victims killed in terrorism attacks 2016	0	35	-	94	15	0	0	-	1	0	7
Foiled Plots 2015	0	0	0	6 - 7	2	3	1	-	0	3	7
Foiled Plots 2016	0	4	0	35	4	0	2	-	1	3	12

Source: Globsec, From Criminals to Terrorists and Back? Kick off Report, 2017.⁶⁹

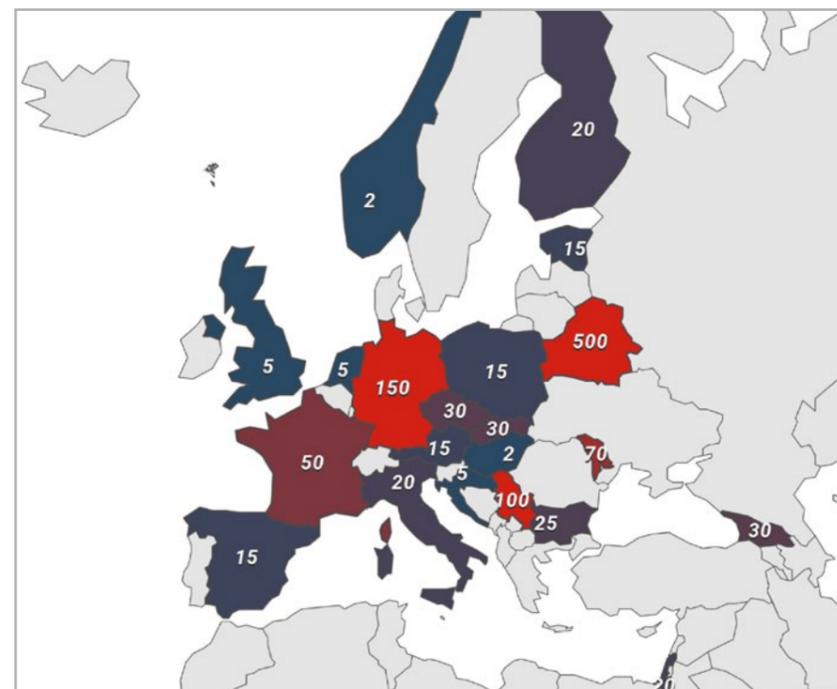
assisted by freedom of expression and freedom of political activity, has also allowed pro-Russian European political parties to organise in opposition to the West and EU.⁷³ These parties even come together in pro-Russian, “patriotically European,”

anti-systemic and far-right coalitions of political activists.⁷⁴ The most radical of this pro-Russian political circle present go further and support pro-Russian separatists and foreign fighters in Eastern Ukraine.⁷⁵



Foreign Fighters fighting on the side of Ukraine 2014-2018 (+ Russian 3,000 FFs)

Source: Arkadiusz Legiec "Profiling foreign fighters in eastern Ukraine: A Theoretical Introduction," in: K. Rekawek (ed.) Not Only Syria? The Phenomenon of Foreign Fighters in a Comparative Perspective. IOS Press, 2017, updated by the author in 2018.⁷⁶



Foreign Fighters in Ukraine fighting on the side of Separatists/Russia 2014-2018 (+ Russian 12,000 FFs)

Source: Ibid.⁷⁷

Russia is also keen on sowing ideological political confusion to undermine the unity and integrity of Transatlantic or European projects. Sowing confusion was clearly on Moscow’s agenda as it expressed, via Russian energy giant Lukoil, an interest in Cambridge Analytica’s now infamous “social media marketing system,” deployed with some success by the Donald Trump and Brexit campaigns.⁷⁸ In this case, a Western invention, Facebook, was effectively weaponised by political insurgents who take pride in disrupting the West’s normal political order of business via activities which dovetailed with Moscow’s efforts to hijack certain political votes in its favour.⁷⁹ Such life changing and modern inventions, just like the freedoms the West cherishes, can and will continue to be utilised against it in the coming years.

Conclusions and recommendations

Transatlantic stakeholders should

- ▶ acknowledge the complex nature of its enemies. These are no longer a single entity or proxies of a single actor, but a collection of oftentimes loosely connected or networked challengers.
- ▶ agree that “it takes a network to defeat a network”. The security challenges facing the West will not lessen and will be multifaceted in nature. Consequently, the West must adapt accordingly, developing and deploying cross departmental capabilities to counter both state and non-state challenges. These could be organised along the lines of the U.S. Army’s Imminent Futures Command, an interdisciplinary “structure implementing modernisation.”⁸⁰
- ▶ Focus on strengthening counterintelligence, with the latter enjoying a much-needed financial boost in key Western or Central European states in recent years. This boost, however, cannot solely be consumed by recruitment drives or technology updates. However, it should be the first step in reorganising Transatlantic intelligence cooperation. In this respect, GLOBSEC’s ideas on reforming Transatlantic counterterrorism, developed by GLOBSEC Intelligence Reform Initiative (GIRI), could be an inspiration for a more networked Western response, namely:

- a) creating permanent hubs that link relevant security specialists;
- b) constructing operational task forces functioning in such hubs to focus on emerging tactical challenges;
- c) developing a federated “hit-no-hit” single search interface that enables each service to proactively seek appendices to data it would be holding;
- d) establishing relevant intelligence centres of excellence to produce common risk assessments, standards and training across the whole transatlantic security community.⁸¹

These recommendations do not constitute silver bullets in the West’s struggle with multifaceted challenges but could open the door to a transformative and 360-degree understanding of security. Such developments would increase the West’s ability to anticipate future threats and strengthen preventive mechanisms present throughout national and multinational security structures. ●

(TREND 5) GLOBAL SECURITY RELATIONS ARE INCREASINGLY CONFRONTATIONAL

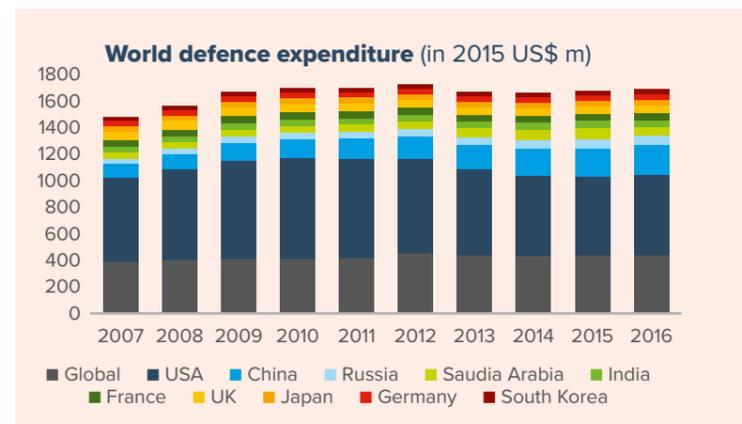
Global security relations are increasingly confrontational. Military budgets are on the rise. Technology offers opportunities for state and non-state actors to acquire powerful weapons. Unresolved conflicts provide ample opportunity for escalation into all-out war.

One of the hitherto observed symptoms of the changing global strategic landscape (i.e. from a unipolar to a multipolar world) has been a continuous and gradual increase of defence expenditures. Last year, global arms spending continued to rise – with every major strategic stakeholder (US, China, India and Russia) increasing defence expenditures on arms, research and technology. The cumulative effect of such expenditures and the spiralling arms race is increasing regional conflict potential.

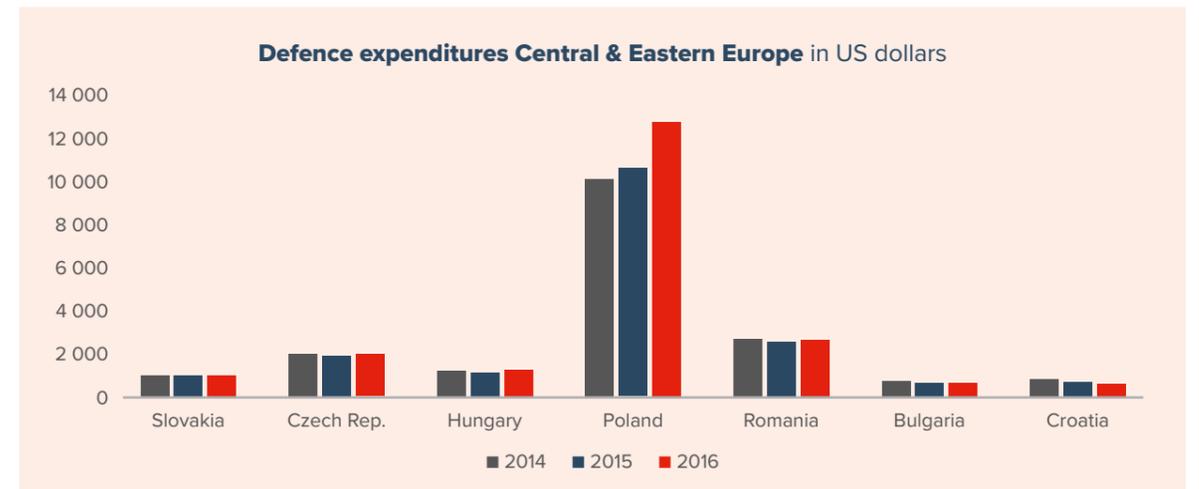
As observed in the final report of the GLOBSEC NATO Adaptation Initiative, NATO’s primary strategic challengers, Russia and China, are seeking to close their capability gap vis-à-vis US technological primacy. In Russia, a constant increase in its warfighting capabilities and a gradual spread of more modern systems has been a constant trend since President Putin’s speech at the 2007 Munich Security Conference.⁸² The 2017 National Security Strategy of the United States which identifies the “growing political, economic, and military competitions” America is “[facing] around the world,” also asks for adequate resources to win these competitions.⁸³ This demand has essentially been met by the spending bill signed in March 2018 which created the basis for the largest military budget (i.e. \$700 billion) in US history.⁸⁴ In China, India and Saudi Arabia, military expenditures have also been breaking historical records and reflect

that these actors are engaged in regional rivalries (the South China Sea, South Asia, the Middle East and North Africa).⁸⁵

Moreover, the elevated spending has been increasingly allocated to a growing variety of defence sectors – including the nuclear and cyber domains. The political tensions between the new US administration of President Donald Trump and ruling regime in Pyongyang have elevated a “dormant” problem into a leading source of global insecurity with notable implications for NATO.⁸⁶ Even in the broader Central European region, the trend of declining military expenditures has been stopped and reversed - most notably by Poland and Romania – with others following suit towards the Defence Investment Pledge (spending at least 2% of GDP on defence) made in 2014. Through the past four fiscal cycles, from 2014 to 2017, the thirteen NATO allies from the CEE region (i.e. the Visegrad, Balkans and Baltic) have increased their cumulative defence spending by a margin of 12% - from \$20,5 billion to \$23 billion.⁸⁷



Source: SIPRI, Military expenditure by country, in constant (2015) US\$ m., 1988-1996, 2017.⁸⁸



Source: North Atlantic Treaty Organization. The Secretary General’s Annual Report 2016, 2017.⁸⁹

Another clear development in the defence sphere is related to the rapid increase in disruptive technology (most prominently: Artificial intelligence and 3D-printing) in weapons systems. This trend holds the critical potential to change the global defence competition as it can shift rivalry from conventional (costly to develop and acquire) capabilities to modern offensive and defensive innovation-driven capabilities. In short, it constitutes another round of strategic offset and shifts competition to a new field in which the past competitive gap of traditionally strong Western actors might be expiring – just like in the 1950s when nuclear weapons were used to avoid a financially crippling “indefinite” conventional arms race, and Airborne Warning and Control System (AWACS), GPS and stealth fighters were used in the 1970s to mitigate the numerical deficit in traditional capabilities.

As a response, all major global actors have been trying to accommodate the shifting reality of the technology driven arms race.⁹⁰ In 2012 the Pentagon’s senior leadership established institutions to address the challenge of developing state-of-the-art weapons and focus on intelligent systems which might replace nuclear and precision-guided weapons as the ultimate guarantor of its security.⁹¹ China, India and other emerging powers have been increasing their innovation potential with direct implications for the defence industry. Only last year, China released an ambitious plan of becoming a global front-runner in AI by 2025

– both economically and militarily.⁹² Vladimir Putin has also proven to be a noticeably vocal proponent of AI as a tool for future power projection, claiming that whoever first masters the immense potential and manages the threats posed by the technology will eventually dominate the global political landscape.⁹³ In the upcoming year, none of the mentioned trends are expected to face a backlash or durable stagnation, as all major actors will continue to pursue their clear long-term strategic objectives.

3D-printing capabilities have been reshaping the global arms landscape even more rapidly. Via its accessible and user-friendly simplified interface, 3D-printing has significantly lowered the bar of technological inputs necessary to develop arms components – essentially it has democratised access to crucial state-of-the-art technology. The areas where 3D printing has direct implications are as diverse as homemade firearms, improvised explosive devices, missile technology and even CBRN (chemical, biological, radiological and nuclear) threats. With further dissemination of the technology, the implications of 3D-printing are likely to grow in the years to come. Take just the most well-known example of the public leak of the first home-made 3D-printed gun blueprint, which was downloaded from the internet by 100,000 users in just two days. As it is essentially unremovable from the internet, the blue-print is available for further downloads, sophistication, testing and evolution.⁹⁴ This trend brings about serious implications for

global security as 3D printers are enabling the production of hard-to-trace non-metallic gun components and materials for sophisticated weapon platforms – such as unmanned aerial vehicles (UAVs) – that completely bypass existing trade regulatory regimes and conventional (legitimate) production supply chains.⁹⁵

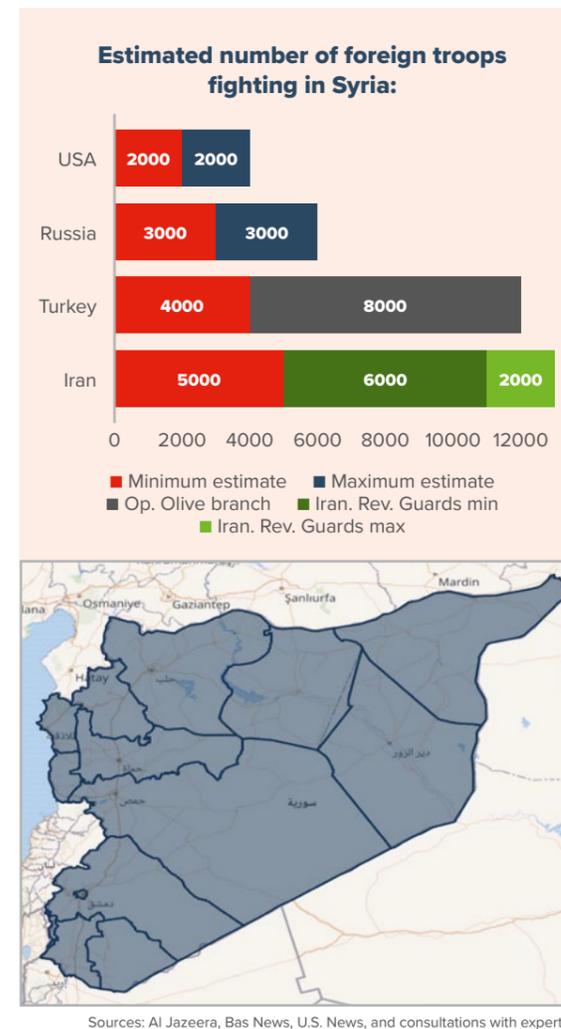
While nuclear arms control stalls, nuclear weapons are being modernized and their engagement threshold is being lowered. Both in the West and the rest of the global system, the latest trends show a clear pattern of “conventionalisation” of nuclear weapons. The trend of the past years has been – despite the rising prominence of new sources of (in)security (for instance cyber capabilities) and continuous investments in conventional weapons – in support of increasing the overall importance of nuclear weapons, with China, the US and Russia announcing future investments into nuclear forces, proving their comparative strategic importance.⁹⁶

In the US, the Trump administration’s aims to pose new nuclear deterrents against Russia and China while simultaneously addressing North Korea’s and Iran’s nuclear ambitions.⁹⁷ For that, the current US administration considers increasing the role of tactical nuclear weapons to widen its spectrum of challenges (from great power balancing to “rogue” state deterrence) to be addressed via nuclear capability. China’s recently acquired capability to place multiple warheads on its ballistic missiles and development of missile submarines and strategic bombers, are a clear sign of the nation’s growing ambitions in the nuclear domain. Although, China’s nuclear arsenal remains small and, for the time being, off alert, its current enrichment potential and procurement activities could enable it to multiply in a small number of annual cycles.⁹⁸ Similarly, Pakistan has been developing an extensive plutonium production capacity in line with light, short-range tactical (battlefield) nuclear weapons – intended to be used in foreseeable battlefield conflict scenarios.⁹⁹ To enhance its second-strike capability, Pakistan has enabled local commanders to launch retaliatory nuclear responses if the survival of the state requires. In India, the military has acquired a full nuclear triad of air-, land- and sea-based nuclear platforms which also includes home-produced nuclear-powered submarines.¹⁰⁰

Last but not least, and most worryingly, Vladimir Putin outlined ambitious plans for a new nuclear-powered cruise missile with unlimited range, an undersea drone with both conventional and nuclear warheads, and an “invincible” air-to-air hypersonic missile.¹⁰¹ In addition, Russia has been begun a production run of short, medium, and long-range nuclear weapons and current estimates count on up to 8000 warheads being developed in the coming decades.¹⁰² Moreover, Moscow has essentially been in violation of the Conventional Arms in Europe (CFE) Treaty, the INF (intermediate range forces) Treaty and its current production trends could soon take the country over the New START Treaty ceiling.¹⁰³

Syria, Yemen and Ukraine remain the main proxy fields of great power competition and regional confrontation. During the Cold War, great power (back then superpower) competition was waged on ideological, industrial and proxy-conflict grounds. Today, as Western values are under attack, arms spending is increasing, and regional/global actors continue to be the playing field of geopolitical rivalry, the situation at times resembles the pre-1989 competition. However, nowadays more actors participate in the world’s great rivalries. In Syria, the US, Russia, Iran, Turkey and Saudi Arabia have been involved in a standoff that has fuelled the country’s destruction. Nonetheless, the proxy warriors still often perceive their clashes as not a “Syrian war,” nor a “Ukrainian war” but “a war between the Russian Federation and the United States.”¹⁰⁴

The interests and operations of international actors in Libya have brought about a lower intensity of conflict that nevertheless follows a similar pattern to Syria. For the likes of Qatar, Turkey, Egypt, UAE and Saudi Arabia, engagement in Libya constituted a tool for supporting the sympathetic regimes for their own strategic interest. At the same time, Russia’s interest in Libya has been aimed at projecting power in a region of critical importance to Western interests. In the broader Middle-East, Saudi Arabia and Iran have been battling each other for regional hegemony for years. The proxy conflict in which this strategic rivalry has taken the most aggressive stance has been Yemen.



In March 2014, war once again returned to Europe, when Russia invaded and seized Crimea and started a proxy war in eastern Ukraine. In return, the European Union and United States responded with punitive economic sanctions against Moscow and limited military assistance to Kyiv. Utilising cyberwarfare and propaganda, Russia has significantly contributed to crippling Ukrainian reform and stability ambitions via a hybrid war which ultimately does not stop at the Ukrainian border but penetrates Western democracies and significantly contributes to eroding post-Cold-War strategic stability. With the election of Russian president Putin, the ongoing freeze in US-Russian relations and lack of a clear political and economic opening by the EU to Ukraine (in the form of a cohesion package, infrastructural development scheme

or enhanced education, science and research initiatives), the conflict in Donbas is unlikely to undergo a notable (positive) shift in the upcoming year and stagnation is likely to remain in place.

Conclusions and recommendations

Transatlantic stakeholders should

- ▶ Search and further develop functional synergies between Allied Western institutions/organisations so as to solidify the West’s approach to key strategic challenges. As the hybrid, cyber and conventional challenges that face European countries do not differentiate between EU or NATO membership, it is thus essential to utilise the toolboxes of both organisations to preserve stability, prosperity and security on the European continent.

- ▶ The West must spend more to bolster its military capabilities, even if that means adopting politically less controversial, but functionally more sensible approaches to defence spending. For example, 30% of 1.5% (of GDP) is more than 20% of 2%, the defence spending target set by NATO Allies - by a margin of 1/10 in real numbers. It is thus more important to invest precious financial resources into the defence budgetary chapters that are directly boosting the warfighting and readiness capabilities of respective countries. Investment in human capital, research and innovation will be key for preserving the West’s competitive military edge on all fronts – i.e. conventional, hybrid, cyber and nuclear.

- ▶ Embrace the opportunities provided by disruptive science and technology to maintain a competitive edge over global rivals. AI, cyber and 3D printing can empower smaller actors across a wider geographical domain. Side-lining ourselves and disregarding the unique market leadership of Western technological companies (and the related innovative know-how) could eventually prove harmful for the Transatlantic community. While embracing disruptive technologies admittedly brings myriad ethical, legal and political challenges, resigning from endorsing them might not prove to be a viable long-term strategy, but a temporary strategic faux-pas. ●

(TREND 6)

UNGOVERNED CYBER SPACE BECOMES AN ALLURING SETTING FOR GLOBAL CONFLICT

According to recent estimates, a business falls victim to a ransomware attack every 40 seconds and this number is predicted to become 14 seconds by 2019.¹⁰⁶ An estimation that is much harder to find is the number of attacks and scale of losses associated with attacks on governmental infrastructure. It is even harder to estimate how many of these attacks are committed or sponsored by other governments, not least because this information, even if proven, is typically kept secret.

With states developing their cyber offensive capabilities on one hand and hiring hackers to carry out stealth cyber-attacks on the other, online space is slowly becoming a battleground for a war where we all stand to be losers. If critical infrastructure attacks become commonplace, countries are faced with the devastating scenario of losing access to basic services like energy and water. Given the high dependence on Information and Communication Technologies (ICTs) and digital networks, the economic damage from such a scenario would be immense and unprecedented.

Proving beyond-any-doubt that a state entity is to blame for a cyber-attack is technologically and legally difficult, to say nothing of potential political confrontations that might spiral out of control. Nonetheless, the trend of publicly attributing attacks to particular states has been accelerating. In the past year alone, the US and UK blamed Russia for a malicious NotPetya attack on Ukraine and businesses associated with the country that spread globally and caused “billions of dollars in damage”.

In another case, the US launched a strong campaign against Iran which involved sanctions and criminal indictments after it was found that the hackers, who attempted to breach universities around the world, were linked to Iran's Islamic Revolutionary Guard Corps and government-funded Mabna Institute.

Public high-profile cases aside, there have been innumerable data breaches, malware insertions, and even attacks on critical services like electrical grids affecting individuals and governments. Currently, almost 4 billion people use the Internet which, coupled with our rapidly increasing dependency on the digital economy, is only set to increase. The adoption of the Internet of Things (IoT) also means that there will be a monumental surge in the number of inter-connected devices.

With the number of potential targets growing daily, governments, lawmakers, private companies, and average users are scrambling to efficiently build up their defences and mitigate damage resulting from such threats. But owing to the decentralized architecture of the Internet which allows easy access and anonymity, those wishing to carry out damage online against an entity, including a government, can do so with relative ease and without geographical considerations, both of which differentiate the online domain from traditional forms of crime. A particularly troublesome point is that there is no playbook for international cyber conflict and warfare. With few, quite unclear, rules regulating cyberspace and, more importantly, with even fewer authorities capable of enforcing them,

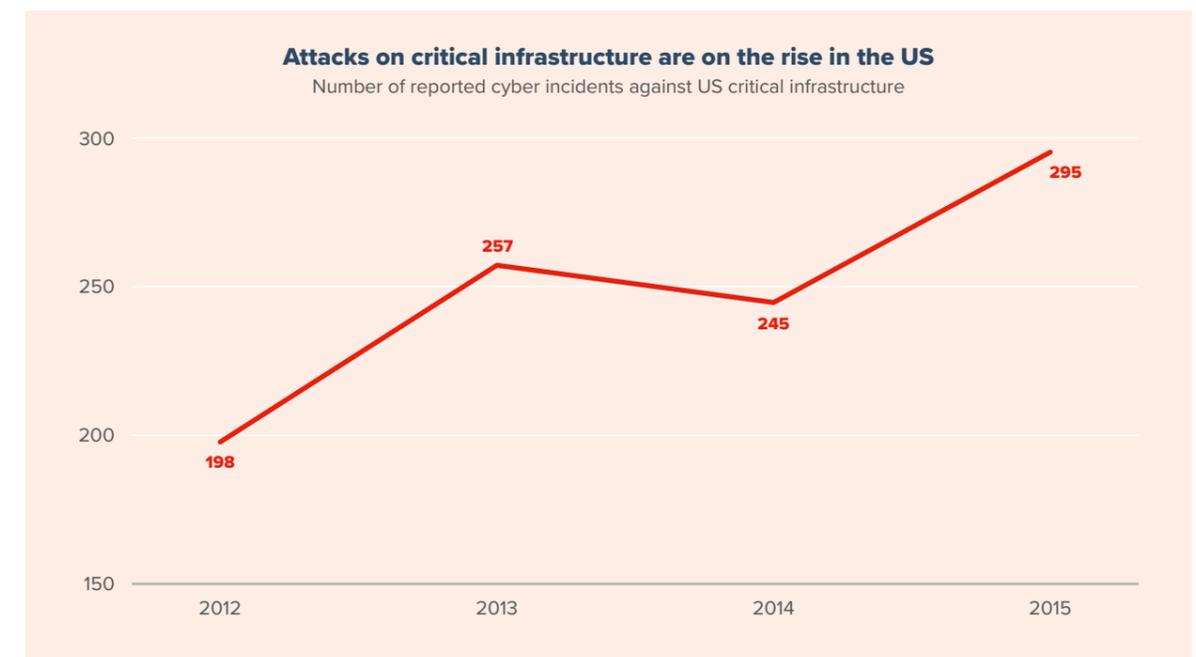
ungoverned cyberspace becomes an alluring setting for global conflicts.

With evidence and indication from almost 30 countries of cyber offensive capabilities, the United Nations has realised the importance of having rules which govern state conduct in cyberspace, just as there are international legal mechanisms for traditional warfare.¹⁰⁷ Therefore, the United Nations Group of Governmental Experts (UNGEE) was set up to establish global norms for cyberspace that should be followed by each state and govern state behaviour. To date, no significant progress towards consensus has been made and 2018 is unlikely to produce a breakthrough.

Consensus on rules for governing cyberspace is difficult to achieve for several reasons, not least because there are differing opinions on whether existing international law can be directly applied or not. Moreover, the divergent approaches to cybersecurity of China and Russia on one side, and the United States and other Western countries on the other, are a thorn in achieving consensus. China and Russia have traditionally focused on cyber sovereignty and information security. Privacy and free flow of communication have not played

a dominant role and the emphasis is placed on limiting citizens' access to the Internet through national regulation and control of content. This is in contrast with the protection of digital networks, privacy and information exchange, and security of hardware and software espoused by the United States.

With intergovernmental platforms failing to govern cyberspace, the role of private tech companies in securing this domain, digital networks, and Internet governance will be significantly higher, both in terms of providing technical tools for cyber defence and establishing global cyber rules. This will be coupled with greater cooperation within the private sector to comprehensively prevent cyber-attacks. The devastatingly high economic damage from cybercrimes will only become higher as emerging technologies like IoT and AI-enabled tools provide the means as well as new avenues for cybercrime networks to use. Microsoft's proposal of the Digital Geneva Convention in 2016 attempted to place the private sector at the forefront of lobbying for a safer cyberspace. More recently, 34 companies including Microsoft and Facebook, signed a 'Cybersecurity Tech Accord' at the RSA conference in San Francisco in April 2018.



Source: Department of Homeland Security, 2015

Economic damage due to cybercrime 2017			
Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
North America	20,2	140 to 175	0,69 to 0,87%
Europe and Central Asia	20,3	160 to 180	0,79 to 0,89%
East Asia & the Pacific	22,5	120 to 200	0,53 to 0,89%
South Asia	2,9	7 to 15	0,24 to 0,52%
Latin America and the Caribbean	5,3	15 to 30	0,28 to 0,57%
Sub-Saharan Africa	1,5	1 to 3	0,07 to 0,20%
MENA	3,1	2 to 5	0,06 to 0,16%
World	\$75,8	\$445 to \$608	0,59 to 0,80%

Source: CSIS & McAfee, Economic Impact of Cybercrime. 2018

Finding themselves without a global framework governing cyberspace and understanding that attacks are likely in such an environment, countries not only accelerate their efforts to improve domestic defences but, when possible, rely on existing allies. In smaller circles of like-minded countries, it becomes easier to establish rules and cooperate on enforcing them. With this logic in mind, NATO has prioritised developing cyber defence capabilities as indicated in their recently-launched Cyber Operations Command Centre with the aim of integrating cyber with its military capabilities. This clear emphasis on coordinated cyber defence trickles down to the country level and is supported by national efforts.

The United States DoD elevated the US Cyber Command to a full-fledged and unified combatant command centre, with President Trump requesting \$647 million for CyberCom in 2018, almost a 16% increase since last year.¹⁰⁸ Similarly, the United Kingdom, has invested almost \$2 billion in enhancing its cyber defence mechanism.¹⁰⁹ It's safe to say that smaller countries that are part of the Alliance will also double up national efforts in the field of cyber defence.

Conclusions and recommendations

► NATO must respond to the challenge of the differing and fragmented cyber capabilities of its Allies so as to build strong cyber deterrence

and, eventually, active cyber defence. Bolstering an exchange of professional military education and cyber defence training both between members and within member states, to harmonise approaches to cyberattacks and threats is needed.

- Governments must prioritise areas within cybersecurity that need an immediate response given the sheer level of damage done to civilians via data breaches, online fraud etc. over the past few years.
- Regional cooperation in the sphere of critical infrastructure protection can be achieved through collaborating on cross-national and sector-specific response planning, especially in the European Union. GLOBSEC has recommended EU member states to urge their national sector-specific protection agencies/regulatory authorities to organize bi-national or regional cyberattack response mechanisms and joint attack response exercises, preferably in forums which engage private sector operators on both sides of the border.¹¹⁰
- The actors involved in shaping as well as regulating the Internet must work together to constantly maintain a strong level of cybersecurity. Responding to cyber threats and building stronger defences is a continuous process which won't be as effective if public and private sector approaches aren't harmonised.

► The private sector must recognise that knowledge-sharing and a common framework of best practices should be encouraged. This helps reduce risk in cybersecurity and is in the best interests of consumers and companies themselves. Protecting external or even internal information systems and devices cannot be a process carried out by one company alone. Intelligence-sharing within financial sector companies in the past, for example, has helped in reducing cybercrime rates. Establishing ISACs (Information Sharing and Analysis Centers) to enable knowledge-sharing in this field, as propagated by ENISA, is important although there are a host of challenges to overcome such as lack of resources and fragmentation of the digital market. ●

(TREND 7) TECHNOLOGIES ARE INCREASINGLY WEAPONISED TO ACHIEVE POLITICAL GOALS

Technological advancements have a distinct set of challenges for societal resilience, stability, and security. As General John Allen stressed in the GLOBSEC NATO Adaptation Initiative Final Report, “the West needs a forward-looking strategy that sets out how we will meet the challenges of an unpredictable and fast-changing world. Technology including artificial intelligence, automation and data analytics represent some of the causes of this unpredictability and pace of changes in today’s world.”

Established institutions in democratic countries are already coping with the consequences of the technology-enabled empowerment of internal and external actors with interests and aims varying from strengthening democracies to overthrowing or destroying them. New technologies augment the impact of social movements, hone political marketing, change the nature of political debate, scale up recruitment for violent causes and enhance coordination of hostile activities.

Social movements around the world are being empowered by technology and that’s both good and bad news. Protests and demonstrations around the Western world – from Romania and Poland to Ireland and the US - are case in point. In Romania, for example, demonstrations began in early 2017 in response to legislation partly decriminalising corruption. Young protesters in one of the European Union’s poorest countries were able to better connect with each other and also promote their activities abroad thanks to reach and impact of social media, putting additional pressure on authorities to investigate high profile corruption cases.¹¹¹ In the United States ideologically

contrasting social movements - students calling for tougher gun control laws after the Parkland school shooting,¹¹² the “Unite the Right” marches¹¹³ of alt-right groups in Charlottesville, Virginia, to name a few – have extensively used social media platforms to organise. So while the Internet itself is simply a tool, it serves as a catalyst, and upgrades one’s ability to mobilise people for a specific cause. Unfortunately, as “Unite the Right” marches illustrate oftentimes such mobilisations further the interests of actors or entities with anti-liberal agendas.¹¹⁴

Political marketing strategies employing machine learning technologies will, in the upcoming years, win elections and shape politics and policies. For more than a decade political campaigns have used tools developed and employed by online marketing agencies to target the right audience with the right messages. This has recently been complemented by the availability and growing understanding of the effects of artificial intelligence, machine learning and big data analytics.

Revelations about Cambridge Analytica, a British data analytics company harvesting personal information of 50 million Facebook users, highlights this growing challenge,¹¹⁵ with experts warning that such practices were previously utilised by other companies and electoral campaigns.¹¹⁶ Such harvests are only made easier by the fact that in 2014 the number of mobile devices exceeded the number of humans. The end result is a situation in which electronic device users today generate 2.5 quintillion (10¹⁸) bytes of data per day.¹¹⁷

With all this data effectively being processed by automated tools, the power of those in possession

of these tools will be one to reckon with. Moreover, and to complicate the issue further, artificial intelligence is also being abused to manipulate public opinion by creating swarms of political bots to spread propaganda and disinformation on all relevant online platforms. The Computational Propaganda Project’s analysis found that traffic about the far-right Alternative für Deutschland (AfD) accounts for a surprisingly large portion of Twitter activity given the party’s share of voter support in Germany.¹¹⁸ The European far-right also mobilises also its followers by deploying armies of botnets (robot networks) sharing anti-EU memes and links to chatrooms with neo-Nazi symbols, Holocaust denial literature and other such materials.¹¹⁹

Bots and Internet trolls continue to pose a threat to political debates in liberal democracies around the world. Bots are autonomous accounts that are programmed to spread political messages that create the illusion of public support, while trolls sow discord by posting highly controversial content. Endorsement by a large number of users elevates consumer trust, reliance, and confidence in the information, and often with little or no attention paid to the credibility of individuals who provided endorsements.¹²⁰ Thus, millions of automated botnets and fake accounts on social media create an assumption that the popularity of a political candidate, an idea or a narrative is much higher than it actually is. In doing so, they create an information and impression bubble and stir public debate or public perception. A growing amount of research proves that Internet trolling, campaigns employing political bots and botnets were prevalent during elections in the United States, France, Germany, Netherlands and Czechia.¹²¹ Research conducted by the University of Southern California also shows that about one in five of the election-related tweets during the last US presidential campaign were generated by bots. The bots supporting Donald Trump outnumbered those supporting Hillary Clinton by more than 3:1, with the Trump bots overwhelmingly tweeting positive sentiments about their candidate.¹²²

As a result, the quality of democracy is in serious jeopardy as those who perfect technology can gain an advantage at the expense of fair electoral processes. The next European Parliament elections

will take place in 2019 and one can expect the trolling campaign on social media to play a large role in the selection of MEPs on both the national and European level. The European Parliament currently consists of 751 MEPs, an estimated 20% of which identify with Euroscepticism or far-right ideology.¹²³

Faced with the growing danger of botnets, liberal democracies need to redefine the rules of the game by clarifying what is legal/illegal and legitimate ways to use specific technologies in political debate while protecting free speech. The abovementioned controversy of Cambridge Analytica, where vulnerabilities in social media platforms were used to influence the outcome of elections or referendums is a taste of the trend we can expect next year and beyond.

While governments are very slow in developing online campaigns, e.g. counter-narratives to extremist online content, there are signs that politicians and officials often make good use of technologies. These include British Conservative Party politicians who utilise WhatsApp, a widely known online communication application, to better coordinate external communications among prominent members.¹²⁴ Such flexible endorsements of new technologies by the traditional mainstream bodes well for the future of democracies as one can expect a Western fightback against challengers in this domain.

On a different note, armed, violent and agile non-state actors increasingly weaponise encrypted communication apps as well as social media platforms to recruit, radicalise and coordinate with new members and followers. Speaking at last year’s Bratislava Forum, GLOBSEC President Róbert Vass stressed that “the Fourth Industrial Revolution, due to its unprecedented speed of system-wide transformation, requires quick understanding of the changing environment and continuous innovation. Non-state actors and businesses are seemingly far more agile and capable of coping with rapid pace and broad impact of the transformation than governments”.¹²⁵

State institutions are gradually adapting to new trends, but they pale in comparison with the

flexibility and energy of non-state actors. And that includes extremist movements as well as terrorists. In this sense, the so-called Islamic State or Daesh sense represents a game changer in the field of effective targeting of vulnerable individuals on various internet platforms for radicalisation and recruitment of new members. The strategic logic of online ISIS propaganda is amplified in the new technology-based communication field, which enables it to shape perceptions and polarise the audience. ISIS has used platforms like Twitter to combat outside influencers and their network adapts at high speeds with limited centralisation. It makes innovative use of platform vulnerabilities that allows them to evade detection or suspension by states.¹²⁶ Their online content output even outperformed many corporate accounts in terms of global outreach. While remote-controlled terrorism, that is directing terrorist attacks from afar and in real time - is by no means a new phenomenon, it is currently more prominent due to the availability of smaller internet platforms with much more sophisticated encryption tools. ISIS recruiters are able to motivate European-born youth¹²⁷ to travel to Syria to join the Caliphate by acting as “virtual planners” providing encouragement and guidance.¹²⁸

Conclusions and recommendations

- ▶ **Technology companies need to establish departments charged with defining the social impact of their products.** These departments should be guided by principles that are transparent and open to public scrutiny.
- ▶ **Governments need to develop close public-private partnerships to counter the online presence and influence of extremist or violent groups.** Exploring options for creating counter-narratives to extremist content online is the first step towards curtailing extremists without interfering with freedom of expression. Such counter-narratives should also be open to external, i.e. public and non-governmental, ideas and inputs.
- ▶ **Governments, ministries and other institutions should hire more “tech-savvy” staff to use the technology to its full potential.** Non-state actors

will most definitely be more agile and energetic than their state counterparts. However, the state should do its best to follow suit and eventually out-perform its challengers.

In line with GLOBSEC’s previous research,¹²⁹ national governments must set up dedicated StratCom capacities, enhance research and the monitoring of information war and its techniques. Countries should develop strategic communication capacities and policies, with StratCom becoming an integral part of national security strategies in a truly interdisciplinary, or cross-departmental, fashion. StratCom cannot be ceded to one authority, body or ministry but necessitates far reaching interest and investments from different national stakeholders. ●

- 1 Vladislava Gubalova, May the Mass Start Begin: The Making of the New EU Budget, GLOBSEC, 2018, <https://www.globsec.org/making-new-eu-budget/>
- 2 Daniel Milo, Katarina Klingová and Dominika Hajdu, GLOBSEC Trends 2017, GLOBSEC Policy Institute, 2017, https://www.globsec.org/wp-content/uploads/2017/09/globsec_trends
- 3 Guillaume Lasconjarias and Tomáš A.Nagy, NATO Adaptation and A2/AD: Beyond the Military Implications, GLOBSEC, 2017, <https://www.globsec.org/publications/nato-adaptation-fa2ad-beyond-military-implications/>
- 4 Kosovo in the 16+1 framework is not regarded as a separate nation-state.
- 5 James Kyngé, Arthur Beesley and Andrew Byrne, EU sets collision course with China over 'Silk Road' rail project, Financial Times, 2017, <https://www.ft.com/content/003bad14-f52f-11e6-95ee-f14e55513608>
- 6 Spectator SME. First trial freight train from China arrives in Bratislava, Spectator SME, 2017, <https://spectator.sme.sk/c/20695576/first-trial-freight-train-from-china-arrives-in-bratislava.html>
- 7 Eszter Zalan. Hungary-Serbia railway launched at China summit, EUObserver, 2017, <https://euobserver.com/eu-china/140068>
- 8 Ivan Krastev, After Europe, University of Pennsylvania Press, 2017
- 9 Lili Bayer, China hits roadblocks in Central Europe, POLITICO, 2017, <https://www.politico.eu/article/china-hits-roadblocks-in-central-europe/>
- 10 Velina Lilyanova, Saudi Arabia in the Western Balkans, European Parliamentary Research Service, 2017, [http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/614582/EPRS_ATAG\(2017\)614582_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/614582/EPRS_ATAG(2017)614582_EN.pdf)
- 11 Filip Rudic, Serbia, Turkey Sign Agreements to Boost Trade, Balkan Insight, 2017, <http://www.balkaninsight.com/en/article/serbia-turkey-sign-agreements-to-boost-trade-10-11-2017>
- 12 Martin Russell, Russia in the Western Balkans, European Parliamentary Research Service, 2017, http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/608627/EPRS_ATAG%282017%29608627_EN.pdf
- 13 International Republican Institute, Bosnia and Herzegovina: Attitudes on Violent Extremism and Foreign Influence, IRI Survey, 2017, http://www.iri.org/sites/default/files/iri_bosnia_poll_february_2017.pdf
- 14 David L. Phillips and Florian Gehajda, Countering Islamic Radicalization and Violent Extremism in Kosovo, Huffington Post, 2017, https://www.huffingtonpost.com/david-l-phillips/countering-islamic-radica_b_9463300.html
- 15 Samet Shabani and Ján Cingel. Working with the Youth: Countering Violent Extremism in Macedonia, GLOBSEC, 2018, <https://www.globsec.org/youth-countering-violent-extremism-macedonia/>
- 16 Daniel Milo, Katarina Klingová and Dominika Hajdu, GLOBSEC Trends 2017, GLOBSEC Policy Institute, 2017, https://www.globsec.org/wp-content/uploads/2017/09/globsec_trends_2017.pdf
- 17 Ivan Krastev, After Europe, University of Pennsylvania Press, 2017
- 18 See Tindemans (1975), Dahrendorf 1979, Wallace and Ridley 1985, Stubb 1996, Schmitter 2000, Hanf 2001, Kolliker 2001, 2006, Holzinger 2012, Fabbri 2015, Fossom 2015, Leruth and Lord 2015, Schimmelfennig et al 2015, Yves Bertoncini 2017
- 19 The Slovak Spectator, Tatra Summit: Multi-speed EU is inevitable, The Slovak Spectator, 2017, <https://spectator.sme.sk/c/20685324/tatra-summit-implies-that-multi-speed-eu-is-inevitable.html>
- 20 John Erik Fossum, Democracy and Differentiation in Europe, Journal of European Public Policy, 22(6), 2015
- 21 European Commission, White Paper on the Future of Europe, COM(2017)2025, 2017, https://ec.europa.eu/commission/sites/beta-political/files/white_paper_on_the_future_of_europe_en.pdf
- 22 Pierre Briançon, France and Germany agree on eurozone reform, Politico, 2018, <https://www.politico.eu/article/french-german-economists-launch-their-own-eurozone-claim/>
- 23 Anne-Sylvaine Chassany, Guy Chazan and Mehreen Khan, France hails progress on plans to strengthen eurozone, Financial Times, 2018, <https://www.ft.com/content/1cb4fea-2ab6-11e8-9b4b-bc4b9f0f381>
- 24 Fiott, Daniel, Antonio Missiroli and Thierry Tardy, Permanent Structured Cooperation: What's in a name?, EU Institute for Security Studies, 2017, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_142_ONLINE.pdf
- 25 Corcoran, Kieran, Almost the entire EU has signed up to a major joint military plan, Business Insider, 2017, <http://uk.businessinsider.com/eu-nations-sign-pesco-joint-military-plan-but-not-britain-2017-11>
- 26 De France, Olivier, Claudia Major and Paola Sartori, How to Make PESCO a Success, Institute for International and Strategic Affairs, 2017, <http://www.iris-france.org/wp-content/uploads/2017/09/Ares-21-Policy-Paper-Sept-2017.pdf>
- 27 Lepiarz, Jacek, Monachium: Morawiecki o UE i NATO, ale wraca sprawa IPN, 2018, <http://www.dw.com/pl/monachium-morawiecki-o-ue-i-nato-ale-wraca-sprawa-ipn/a-42627884>
- 28 G.J. Ikenberry, The Future of Multilateralism: Governing the World in a Post-Hegemonic Era, Japanese Journal of Political Science, 2015
- 29 J.D. Colgan, R.O. Keohane, The Liberal Order Is Rigged, Foreign Affairs, May/June 2017
- 30 R. Harte, Multilateralism in international trade: WTO achievements and challenges, EP Think Tank, 7 December 2017
- 31 IMF Data Mapper (13/04/2018) <http://www.imf.org/external/datamapper/NGDPD@WEO/WEOORLD>
- 32 About the Inclusive Framework on BEPS, BEPS Composition 2018, the OECD.
- 33 <https://www.cfr.org/blog/president-trump-and-future-global-governance>
- 34 M. Eilstrup-Sangiovanni, The Global Crisis of Multilateralism, E-International Relations, 3 December 2016.
- 35 E. Lazarou, The future of multilateralism. Crisis or opportunity?, European Parliamentary Research Service, PE. 603.922, May 2017
- 36 T. Mitchell, Sh. Donnan, Chinese trade chiefs scan Washington for elusive dealmakers, the Financial Times, 7 April 2018
- 37 US-China trade tariffs in charts <https://www.ft.com/content/e2848308-3804-11e8-8eee-e06bde01c544?imgagelid=271347fc-3823-11e8-8b98-2f31af407cc8>
- 38 M. Rostowska, Trade Agreements across the Atlantic: What Lessons from CETA for TTIP?, PISM Strategic File No. 9 (36), December 2013
- 39 K. Stokes, "Brexit vote highlighted UK's discontent with EU, but other European countries are grumbling too", Pew Research Centre, 24 June 2018, <http://www.pewresearch.org/fact-tank/2016/06/24/brexit-vote-highlighted-uks-discontent-with-eu-but-other-european-countries-are-grumbling-too/>
- 40 J.D. Colgan, R.O. Keohane, The Liberal Order Is Rigged, Foreign Affairs, May/June 2017
- 41 W. Russel Mead, The Jacksonian Revolt: American Populism and the Liberal Order, Foreign Affairs, March/April 2017
- 42 K. Brudzinska, Bridges Instead of Walls? – Not So Easy, Blog, Globsec Policy Institute, 17 February 2017,
- 43 K. Brudzinska, M. Rostowska, North America's New Trade Deals: From NAFTA to TTP and TTIP, PISM Bulletin, 18 February 2013
- 44 Pacific nations would welcome US back to TPP, the Financial Times, 13 April 2018
- 45 Cars block the road to a renegotiated NAFTA, the Economist, 1 February 2018
- 46 T. Mitchell, Sh. Donnan, Chinese trade chiefs scan Washington for elusive dealmakers, the Financial Times, 7 April 2018
- 47 US-China trade tariffs in charts <https://www.ft.com/content/e2848308-3804-11e8-8eee-e06bde01c544?imgagelid=d4936a82-380b-11e8-8b98-2f31af407cc8>
- 48 U. Dadush, U.S. steel and aluminium tari s: how should the EU respond?, Blob Bruegel, 9 March 2018,
- 49 "Trade war brewing? World Trade in 2018", the Economist Intelligence Unit 2018, www.eiu.com/public/topical_report.aspx?campaignid=WorldTrade2018
- 50 Cutting aid and diplomacy will make America weaker, the Economist, 23 March 2017
- 51 Congressional Budget Justification, Foreign Assistance, Supplementary Tables, Fiscal Year 2018, <https://www.state.gov/documents/organization/271014.pdf>
- 52 E. Lazarou, The future of multilateralism. Crisis or opportunity?, European Parliamentary Research Service, PE. 603.922, May 2017
- 53 The European Union at the United Nations, fact sheet, Major Contributions, 14 September 2017.
- 54 As the world sours on trade, the EU sweetens on it, the Economist, 30 March 2017
- 55 "Full details of the EU's ongoing trade negotiations." The European Commission, March 2018, trade.ec.europa.eu/doclib/docs/2006/december/tradoc_118238.pdf.
- 56 Ibidem
- 57 Strategy for the Western Balkans, The European Commission, 8 February 2018
- 58 <https://www.globsec.org/wp-content/uploads/2017/11/GNAI-Final-Report-Nov-2017.pdf>, p. 6.
- 59 <https://www.thelocal.it/2017/11/03/italian-police-seize-isis-drugs>
- 60 <https://www.theguardian.com/world/2014/jun/29/isis-iraq-caliphate-declaration-war>
- 61 K. Klingova, T. Nagy, Paramilitarne Skupiny v Krajinach V4. Hrozba Alebo Prilezitost?, GLOBSEC, Bratislava 2017.
- 62 <http://abcnews.go.com/Blotter/al-qaeda-promises-us-death-thousand-cuts/story?id=12204726>
- 63 See: <https://www.globsec.org/wp-content/uploads/2017/12/Crime-Crime-Terror-Nexus-update.pdf>
- 64 <https://www.globsec.org/wp-content/uploads/2017/11/GNAI-Final-Report-Nov-2017.pdf>, pp. 6, 10.
- 65 <http://www.independent.co.uk/news/world/middle-east/isis-ramadan-2017-all-out-war-west-new-terror-attacks-manchester-suicide-bombing-islamic-state-a7758121.html>
- 66 <http://smallwarsjournal.com/jrn/art/the-united-states-and-russia-are-already-at-war>
- 67 <https://inmoscowshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>
- 68 <https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html>
- 69 https://www.washingtonpost.com/news/worldviews/wp/2018/01/20/the-pentagon-says-china-and-russia-are-bigger-problems-for-u-s-than-terrorists-american-voters-may-not-agree/?utm_term=.0f520124abf7
- 70 See: D. Golden, Spy Schools: How the CIA, FBI, and Foreign Intelligence Secretly Exploit America's Universities, New York: Henry Holt and Co., 2017.
- 71 <https://euobserver.com/foreign/137743>
- 72 <https://www.telegraph.co.uk/news/2018/03/17/moscow-expel-23-british-diplomats-row-russian-involvement-spy/>
- 73 See: <https://www.amazon.com/Black-Wind-White-Snow-Nationalism/dp/0300226454>
- 74 <http://www.dw.com/en/pegida-meets-with-european-allies-in-the-czech-republic/a-19000895>
- 75 https://www.pism.pl/files/?id_plik=19434
- 76 See Arkadiusz Legieć in Not Only Syria? The Phenomenon of Foreign Fighters in a Comparative Perspective. edited by K. Rekawek, table updated on 1st March 2018.
- 77 Ibid.
- 78 <https://www.theguardian.com/news/2018/mar/17/cambridge-academic-trawling-facebook-had-links-to-russian-university>
- 79 <https://www.amazon.com/Collusion-Secret-Meetings-Russia-Helped/dp/0525562516>
- 80 <https://www.defensenews.com/land/2018/02/08/army-futures-command-might-be-in-a-city/>
- 81 <https://www.globsec.org/initiatives/globsec-intelligence-reform-initiative/>
- 82 See: <https://www.youtube.com/watch?v=hQ58Yv6kP44>.
- 83 See: The President of the United States, National Security Strategy of the United States of America, December 2017, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.
- 84 Lendon, Bred. What the massive military budget pays for, CNN Politics, March 28, 2018. <https://edition.cnn.com/2018/03/28/politics/us-military-spending-items-intl/index.html>
- 85 SIPRI, Military Expenditures Database for 2017, 2017. <https://www.sipri.org/sites/default/files/Milex-constant-2015-USD.pdf>
- 86 Nagy, Tomas A. Central Europe at War with North Korea, The Diplomat, March 12, 2018. <https://thediplomat.com/2018/03/thinking-the-unthinkable-central-europe-at-war-with-north-korea/>
- 87 North Atlantic Treaty Organization. The Secretary General's Annual Report, p.110. March 15, 2018.
- 88 SIPRI, Military expenditure by country, in constant (2015) US\$ m., 1988-1996, 2017.
- 89 North Atlantic Treaty Organization. The Secretary General's Annual Report 2016, March 13, 2017.
- 90 Osoba, Osonde A. and William Welser, The Risks of Artificial Intelligence to Security and the Future of Work, RAND Corporation, p.16, 2017.
- 91 McLeary, Paul. The Pentagon's Third Offset May Be Dead, But No One Knows What Comes Next, Foreign Policy, December 18, 2017. <http://foreignpolicy.com/2017/12/18/the-pentagons-third-offset-may-be-dead-but-no-one-knows-what-comes-next/>
- 92 Allen, Gregory C., China's Artificial Intelligence Strategy Poses a Credible Threat to U.S. Tech Leadership, Council on Foreign Relations, December 4, 2017. <https://www.cfr.org/blog/chinas-artificial-intelligence-strategy-poses-credible-threat-us-tech-leadership>
- 93 Meyer, David. Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World, Fortune magazine, September 7, 2017. <http://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/>
- 94 Greenberg, Andy. 3D-printed Guns Blueprints Downloaded 100000 Times, Forbes. 5 July, 2013, <http://www.forbes.com/sites/andygreenberg/2013/05/08/3d-printed-guns-blueprints-downloaded-100000-times-in-two-days-with-some-help-from-kim-dotcom/>.
- 95 Lindstrom, Gustav. Why should we care about 3D-printing and what are potential security implications? Geneva Center for Security Policy, September 2014.
- 96 Sanger, David and William Broad, To Counter Russia, U.S. Signals Nuclear Arms Are Back in a Big Way, New York Times, February 4, 2018. <https://www.nytimes.com/2018/02/04/us/politics/trump-nuclear-russia.html>
- 97 Dews, Fred. 2018 Nuclear Posture Review tailored to 21st century threats, Brookings Institution, February 16, 2018.
- 98 Tsuruoka, Doug. Is China Really Threatening America with Nuclear Weapons? The National Interest, February 20, 2018.
- 99 Gul, Ayaz, Pakistan Enhances Range of Controversial 'Tactical' Nuclear Weapon, Voice of America, July 5, 2017, <https://www.voanews.com/a/pakistan-enhances-range-of-controversial-tactical-nuclear-weapon/3929249.html>
- 100 Rajeev, Nishant. A Holistic Approach to India's Nuclear Doctrine, The Diplomat, May 24, 2017, <https://thediplomat.com/2017/05/a-holistic-approach-to-indias-nuclear-doctrine/>
- 101 Hennigan, W.J. Why Vladimir Putin's 'Invincible' Missile Claim Comes at a Bad Time, Time Magazine, March 2 2018. <http://time.com/5182159/russia-Invincible-missile-nuclear-weapons/>
- 102 Blank, Stephen. Getting Russia's Nuclear Strategy Mostly Right, The Hill, February 25, 2018. <http://thehill.com/opinion/international/375340-getting-russias-nuclear-strategy-mostly-right>
- 103 Schneider Mark B., Russian Violations of the INF and New START Treaties, Real Clear Defence, August 15, 2016. https://www.realcleardefense.com/articles/2016/08/16/russian-violations_of_the_inf_and_new_start_treaties_109708.html
- 104 Khazov-Cassia, Sergei and Robert Coalson, Russian Mercenaries: Vagner Commanders Describe Life Inside The 'Meat Grinder', Radio Free Europe / Radio Liberty, March 14, 2018. <https://www.rferl.org/a/russian-mercenaries-vagner-commanders-syria/29100402.html>
- 105 Various online sources: <http://www.basnews.com/index.php/en/news/middle-east/395330>, <https://www.aljazeera.com/news/2017/12/syria-doubts-putins-russian-troop-exit-claim-171212173616788.html>, <https://www.usnews.com/news/world/articles/2017-01-11/turkey-bogged-down-in-syria-as-it-realigns-with-russia-and-consultations-with-kyle-orton>
- 106 Morgan, S 2017 Cybercrime Report, Cybersecurity Ventures <https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>
- 107 <https://public.tableau.com/profile/diplotofoundation#!/vizhome/Offensivecybercapabilities/Offensivecybercapabilities?publish=yes>
- 108 Pomerleau, M., "CyberCom Elevation at Heart of Budget Increase", 24 May, 2017 <https://www.defensenews.com/2017/05/24/cybercom-elevation-at-heart-of-budget-increase/>
- 109 Gross, G "UK government to spend 2.3 billion to bolster cybersecurity", 1 November, 2016 <https://www.pcworld.com/article/3137161/security/uk-government-to-spend-2-3-billion-to-bolster-cybersecurity.html>
- 110 <https://www.globsec.org/publications/good-neighbors-make-good-security-coordinating-eu-critical-infrastructure-protection-cyber-threats/>
- 111 C. Fishwick. "'27 years of corruption is enough': Romanians on why they are protesting." The Guardian. 6 February 2017. <https://www.theguardian.com/world/2017/feb/06/27-years-of-corruption-is-enough-romanians-on-why-theyre-protesting> (accessed 20.3.2018).
- 112 J. E. Bromwich. "How the Parkland Students Got So Good at Social Media." 7 March 2018. <https://www.nytimes.com/2018/03/07/us/parkland-students-social-media.html> (accessed 21.3.2018).
- 113 F. Diep. "How Social Media Helped Organize And Radicalize America's White Supremacists." 15 August 2017. <https://psmag.com/social-justice/how-social-media-helped-organize-and-radicalize-americas-newest-white-supremacists> (accessed 21.3.2018).
- 114 Erin Marie Saltman. "How young people join violent extremist groups – and how to stop them, TEDxGhent, https://www.ted.com/talks/erin_marie_saltman_how_young_people_join_violent_extremist_groups_and_how_to_stop_them (accessed 20.3.2018).
- 115 C. Cadwalladr. E. Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach." The Guardian. 17 March 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election?CMP=fb_gu (accessed 20.3.2018).
- 116 C. Miller, "The big business of disinformation." Wired. 10 June 2017. <http://www.wired.co.uk/article/carl-miller-disinformation-gets-commercialised> (accessed 21.03.2018).
- 117 McKinsey&Company. "McKinsey Analytics, An executive's guide to AI." <https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/an-executives-guide-to-ai> (accessed 16.3.2018)
- 118 L.M. Neudert, B. Kollanyi P. N. Howard. "Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?" Data Memo 20177. Oxford, UK: Project on Computational Propaganda. <http://comprop.oii.ox.ac.uk/research/junk-news-and-bots-during-the-german-parliamentary-election-what-are-german-voters-sharing-over-twitter/> (accessed 20.3.2018)
- 119 B. Nimmo. "#ElectionWatch: Russian Botnet Boosts German Far-Right Posts, Digital Forensic Research Lab, Atlantic Council, <https://medium.com/dfrlab/german-election-russian-botnet-boosts-far-right-posts-45f170bc2321> (accessed 21.3.2018)
- 120 Ch. Paul, M. Matthews. "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It." RAND Corporation 2016. https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf (accessed 21.3.2018).
- 121 D. Ghosh, B. Scott. "Russia's Election Interference Is Digital Marketing 101." The Atlantic. 19 February 2018. <https://www.theatlantic.com/international/archive/2018/02/russia-trump-election-facebook-twitter-advertising/553676/> (accessed 21.3.2018); "Russia Attempted to Influence French and Dutch Elections With Suspect Polls." Bellingcat. 6 June 2017. <https://www.bellingcat.com/news/uk-and-europe/2017/06/06/russia-attempted-influence-french-dutch-elections-suspect-polls/> (accessed 21.3.2018); L. Gyori, et al. "Does Russia Interfere in Czech, Austrian and Hungarian Elections?. Political Capital, European Values Think-tank, DoW. 2017. http://www.politicalcapital.hu/pc-admin/source/documents/western_experiences_eastern_vulnerabilities_20170102.pdf (accessed 21.3.2018).
- 122 A. Bessi, E. Ferrara. "Social Bots Distort the 2016 U.S. Presidential Election Online Discussion." First Monday Journal, Vol. 21, No. 11, Nov. 7, 2016. http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653?utm_content=buffer37108&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#author (accessed 21.3.2018).
- 123 M. Apelblat. "How do we face extremists in the EU Parliament?." Euractive. 2 June 2014. <https://www.euractiv.com/section/eu-elections-2014/opinion/how-do-we-face-extremists-in-the-eu-parliament/> (accessed 16.3.2018).
- 124 See: T. Ross, T. McTague. "Betting the House: The Inside Story of the 2017 Election. London: Biteback Publishing, 2017.
- 125 R. Vass at GLOBSEC 2017 Bratislava Forum, 28 May 2017
- 126 J. Shaheen. "Network of Terror, How Daesh uses adaptive social networks to spread its message." StratCom. Center of Excellence. November 2015. <https://www.stratcomcoe.org/download/file/fid/3312> (accessed 16.3.2018).
- 127 "Syria girls: First missing London schoolgirl names." BBC. 14 March 2015. <http://www.bbc.com/news/uk-31886146> (accessed 16.3.2018).
- 128 S. Mullins. "Lone Actor Vs. Remote-Controlled Jihad: Terrorism: Rethinking The Threat To The West." War on the Rocks. 20 April 2017. <https://warontherocks.com/2017/04/lone-actor-vs-remote-controlled-jihadi-terrorism-rethinking-the-threat-to-the-west/> (accessed 20.3.2018).
- 129 D. Milo, K. Klingová. "Countering Information War, Lessons Learned from NATO and Partner Countries." GLOBSEC 2017. https://www.globsec.org/wp-content/uploads/2017/09/countering_information_war.pdf (accessed 21.3.2018).



► Polus Tower II
Vajnorská 100/B
831 04 Bratislava
Slovak Republic



► +421 2 3213 7800
► info@globsec.org
► www.globsec.org