VOLUME 8, ISSUE 2, 2017

per Concordiam

Journal of European Security and Defense Issues

- **CROSS-BORDER MEDDLING**
  Russia's fixation on regional power
- **MANAGING DIVERSITY**
  Tolerance builds stronger states
- **LEGISLATING CYBER WARFARE**
  Current laws are inadequate
- **WINNING THE INFORMATION WAR**
  How to marginalize hostile propaganda

PLUS

Turkey's ISIS response
Multistate cyber security operations
An assault on drug trafficking

THE SURVIVAL OF ENLIGHTENED STATES

Protecting the Homeland

features

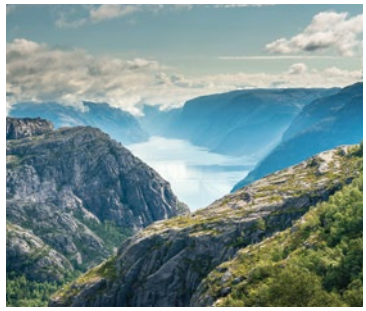
departments

in every issue

COOPERATION

SECURITY

POLICY



on the cover:

Lysefjord in Norway provides a tranquil scene in a world where global threats are a growing concern. ISTOCK

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the 30th issue of *per Concordiam*. In this issue, we look at developing strategies to address the challenges of "resiliency" at the nation/state level. In this context, resiliency represents a nation's ability to provide stability to its citizens, thereby protecting itself from both internal and external threats. Resilience comes from within a country, through rule of law, good governance, a competitive media system, checks and balances, and transparent and functioning institutions. Our authors provide excellent examples of these characteristics.

Pál Dunay and Besa Kabashi-Ramaj examine the present-day global security context, including the conflict between states that would prefer a return to the Westphalian international order of state sovereignty and those that desire a post-Westphalian world where states, societies and people interact freely. Andreja Durdan writes about the challenges posed by managing diversity, which is difficult even for established democracies because of the increasing permeability and fluidity in a globalized world.

Dr. Stefan Meister argues that sustained economic and democratic development throughout the European region is a function of each state's capacity to provide security to its citizens and improve statehood through functioning institutions grounded in the rule of law. Dr. Ieva Bērziņa develops the idea that an effective resistance to the influence of hostile foreign information requires the winning of the hearts and minds of the home audience based on the belief that a state's weakness in terms of state and societal relations should be of greater concern than the strength of its opponents.

The Marshall Center's objective is to share effective methods, learn from each other and discuss emerging trends to learn how the European Union and NATO can formulate new southern flank strategies while minimizing negative spillovers and "collateral damage" to NATO and EU neighbors and partners. I hope the ideas in this issue increase dialogue on this complicated but important topic and help inform EU and NATO strategic thinking.

As always, we at the Marshall Center welcome your comments and perspectives on these topics and will include your responses in future editions. Please feel free to contact us at editor@perconcordiam.org

Sincerely,

Keith W. Dayton
Director

Keith W. Dayton

Director, George C. Marshall European Center for Security Studies

Keith W. Dayton retired as a Lieutenant General from the U.S. Army in late 2010 after more than 40 years of service. His last assignment on active duty was as U.S. Security Coordinator to Israel and the Palestinian Authority in Jerusalem. An artillery officer by training, he also has served as politico-military staff officer for the Army in Washington, D.C., and U.S. defense attaché in Russia. He worked as director of the Iraqi Survey Group for Operation Iraqi Freedom in Iraq. He earned a Senior Service College Fellowship to Harvard University and served as the Senior Army Fellow on the Council on Foreign Relations in New York. Gen. Dayton has a bachelor's degree in history from the College of William and Mary, a master's degree in history from Cambridge University and another in international relations from the University of Southern California.

Dr. Ieva Bērziņa is a senior researcher at the Center for Security and Strategic Research, National Defence Academy of Latvia. Her current research includes Russian information warfare, "colour revolutions," the rhetoric of political leaders, political marketing and strategic communication.

Pál Dunay, Ph.D., is a professor of NATO and European security issues at the Marshall Center. He was course director of the international training course in security policy at the Geneva Centre for Security Policy, 1996-2004 and 2007-2014. He was senior researcher at the Stockholm International Peace Research Institute, 2004-2007, and director of the Organization for Security and Co-operation in Europe Academy in Bishkek, Kyrgyz Republic, 2014-2016. His primary research interests include the former Soviet Union, east central Europe and European security more broadly.

Andreja Durdan is an intelligence officer in the Security Intelligence Agency, Croatia. Previously, she worked in the Ministry of Interior. She is a 2014 graduate of the Marshall Center's Program in Applied Security Studies and holds a master's degree in economics from the Faculty of Economics and Business, University of Zagreb, Croatia.

Klaus-Dieter Fritsche is state secretary at the German Federal Chancellery and German commissioner for the Federal Intelligence Services. He has served in the German security sector for more than 20 years, including as state secretary at the Federal Ministry of the Interior, director-general for federal services at the Federal Chancellery and vice president of the Federal Office for the Protection of the Constitution. He holds a state examination in law.

Dr. Sven Bernhard Gareis has served as German deputy dean at the Marshall Center since 2011. He was previously deputy head of the faculty of humanities and social sciences at the Führungsakademie der Bundeswehr in Hamburg for five years. He remains a professor of international politics at the Westfälische Wilhelms-Universität in Münster and has taught as a visiting professor at the Hebrew University in Jerusalem and Tamkang University in Taiwan.

Besa Kabashi-Ramaj is the director of the Centre for Research Documentation and Publication. She is the founder and owner of B.K.R. & Associates, and serves as an adviser on national security issues to the prime minister of Kosovo. She has more than 10 years of experience in the areas of management, policymaking, international security, national security and defense reform, military affairs and public information and holds a master's degree in public and international affairs/security and intelligence from the University of Pittsburgh in the United States.

Dr. Stefan Meister leads the Robert Bosch Center for Central and Eastern Europe, Russia and Central Asia at the German Council on Foreign Relations. He was a senior policy fellow at the European Council on Foreign Relations and a visiting fellow at the Transatlantic Academy in Washington, D.C. He specializes in Russian domestic, foreign and energy policy; the interrelationship between Russian domestic and foreign policy; and post-Soviet conflicts, particularly in the South Caucasus. He co-authored *The Eastern Question: Russia, the West and Europe's Grey Zone,* published by Brookings Institution Press (2016).

per Concordiam
Journal of European Security and Defense Issues

Survival of the State

Volume 8, Issue 2, 2017

George C. Marshall European Center for Security Studies

Leadership

Keith W. Dayton
Director

Ben Reed
U.S. Deputy Director

Johann Berger
German Deputy Director

Ambassador Douglas Griffiths
International Liaison

Marshall Center

The George C. Marshall European Center for Security Studies is a German-American partnership founded in 1993. The center promotes dialogue and understanding between European, Eurasian, North American and other nations. The theme of its resident courses and outreach events: Most 21st century security challenges require international, interagency and interdisciplinary response and cooperation.

Contact Us

per Concordiam editors
Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
editor@perconcordiam.org

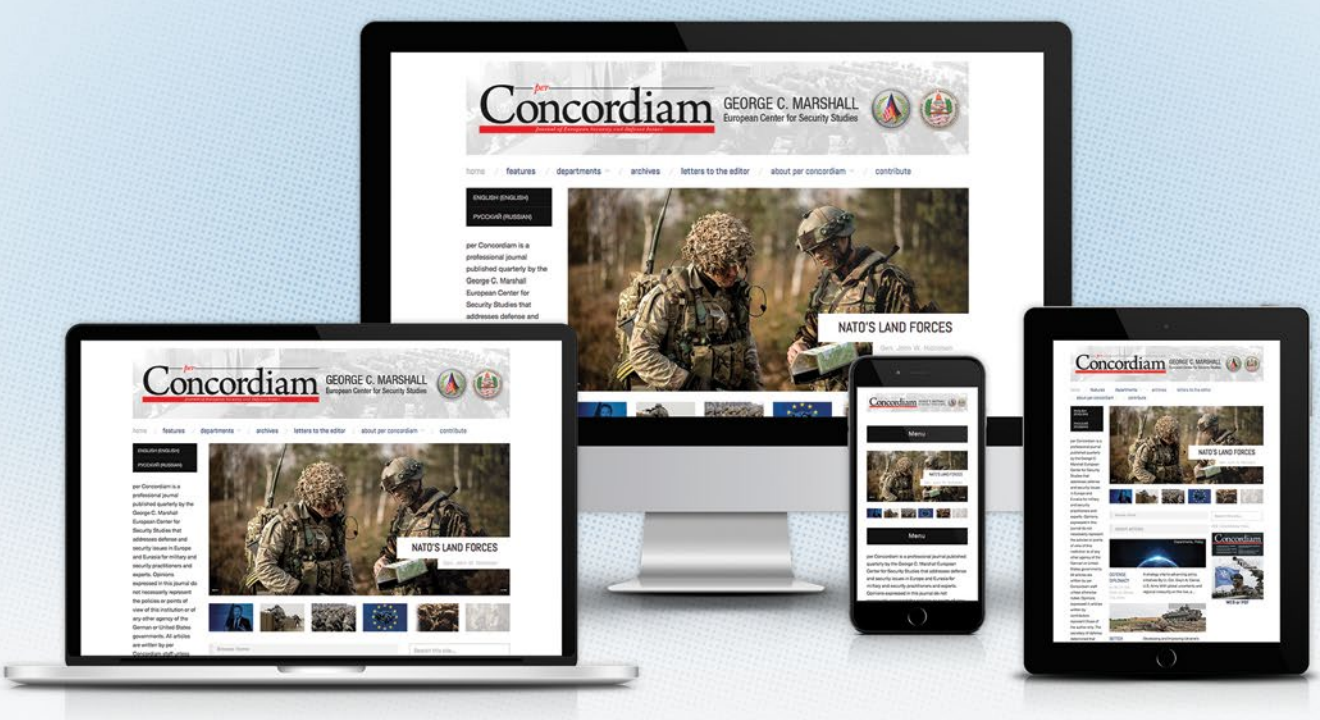
ISSN 2166-322X (print)
ISSN 2166-3238 (online)

A DOUBLE DOSE
ONLINE

Read current and past issues of *per Concordiam*

http://perconcordiam.com

Submit articles, feedback and subscription requests to the Marshall Center at: editor@perconcordiam.org



Get the freshest *global security news* updated weekly:

transnational weekly

http://www.marshallcenter.org

GEORGE C. MARSHALL EUROPEAN CENTER FOR SECURITY STUDIES
DEMOCRATIA PER FIDEM ET CONCORDIAM

Hybrid THREATS

Coping with new challenges

By **KLAUS-DIETER FRITSCHE**, state secretary at the German Federal Chancellery, German commissioner for the Federal Intelligence Services

With the end of confrontation between East and West came a long period when it seemed that peace and security in Europe could be taken for granted. American political scientist Francis Fukuyama even claimed in his book, *The End of History and the Last Man*, that the end of the Cold War marked the end of the era of great conflicts.

But events took a different turn, and over the past few years the world has become more chaotic. A tectonic shift in classical geopolitics is tearing apart the stability, continuity and security of states and entire regions. For the West, long-standing certainties about security policy have been replaced by a multitude of challenges in Afghanistan, Syria, Iraq and Libya, and by Russia's more assertive foreign policy, the war in the east of Ukraine, China's new self-confidence and the refugee crisis.

Additionally, the West faces a new security challenge. In a 1993 study, John Arquilla and David Ronfeldt predicted the coming of cyber war, which is now a reality. The term, however, is somewhat vague and often used in a context that goes well beyond its original meaning. It initially referred to military operations involving information technology. Today, the term encompasses all attacks on cyber security, such as cyber espionage or cyber crime.

But in both its original meaning and its broader definition, cyber war exemplifies the phenomenon of "hybrid threats," another term that, along with cyber war, has become part of our everyday language. These threats pose new challenges that reside at the meta-level and encompass hidden aggressions by state and nonstate actors against private individuals, companies, authorities and governments. The attacks are hard to identify and difficult to trace. They originate in the anonymity of the web and are carried out through traditional or electronic media or involve military or intelligence services acting incognito. The antagonists make it difficult for defenders to detect and repel attacks while adhering to international conventions.

Attacks on cyber security, targeted disinformation, spin and propaganda are now a reality. Preventing the misuse of digital technologies is a primary challenge of the 21st century. Cyber attacks on critical infrastructure such as energy supply, telecommunications, airports, roads and railroads, financial institutions, political parties or government agencies can destabilize countries, influence elections or overthrow governments. Disruptions, manipulations, sabotage and targeted attacks on electronic networks are the side effects of the information society.

Another common term, in the context of cyber security, is cyber espionage, which threatens the privacy of individuals, companies and state agencies. German companies lose an estimated 50 billion euros annually to cyber espionage. The massive cyber attack on the internal network of the German Bundestag, uncovered in May 2015, demonstrated most dramatically the vulnerability of state agencies.

The German Federal Chancellery building in Berlin ISTOCK

The enormous impact of complex cyber attacks on states became evident in Estonia in 2007. An unprecedented attack on the Baltic state paralyzed banks, government agencies, police and government for days. The attack occurred while the Estonian government was locked in a dispute with Russia over the relocation of a Soviet-era military memorial within the city of Tallinn, leading to speculation that Russia was responsible, though the Estonian Computer Emergency Response Team could never positively identify the attackers. So it is no coincidence that NATO established its Cooperative Cyber Defence Centre of Excellence in Estonia. Based in an old garrison in Tallinn, the center is the knowledge hub — the "brain" — in the fight against cyber espionage and digital terrorism in Europe. This is where, once a year, NATO members hold a real-time network defense exercise with expert teams that practice ways to support a state hit by massive cyber attacks.

In Brussels, the European Union runs the Intelligence and Situation Centre, an analysis hub for its members' intelligence services. In 2016, the center activated its unit for hybrid threats, the Hybrid Fusion Cell. It issues early-warning reports and cooperates with agencies such as the Cybercrime Center and the Counter Terrorism Center at Europol's headquarters, and with Frontex (the European Border and Coast Guard Agency) and the EU's Computer Emergency Response Team.

Hybrid attacks overstep the limits of what is perceived as "legitimate means of foreign policy." They remain below the threshold of conventional war but nevertheless represent serious attacks on societies. Democracies based on the rule of law find it difficult to adopt effective countermeasures because there is no "equality of arms." Western democracies comply with laws and play by the rules; hybrid attackers avoid them intentionally. In any case, countermeasures by states or EU institutions require resolve and cohesion.

But even at the domestic level, confronting cyber attacks is an extremely complex challenge. In democracies, state agencies operate within clearly defined areas of jurisdiction and competence. But the phenomenon of hybrid threats cannot be subdivided into domains that neatly coincide with the state agencies' areas of competence. It is a gray zone in which law enforcement, intelligence and information technology security agencies need to cooperate.

Each agency assesses an incident from its own angle and acts on the basis of its jurisdiction and competence. Because of Germany's federal structure, jurisdiction is divided between the federal government and its states. Not only is the Federal Office for the Protection of the Constitution in charge of counterespionage, but so are the 16 State Offices for the Protection of the Constitution. Law enforcement is not only the responsibility of the

Federal Criminal Police Office, but also of the 16 State Offices of Criminal Investigation. This uniquely German approach adds to the challenges of countering cyber attacks because greater coordination is required to fight a phenomenon that knows no boundaries.

To cope with such challenges, Germany opted for the whole-of-government approach. In 2011, the federal government published its first cyber security strategy. As a result, the National Cyber Defence Centre was founded. Here, all the agencies involved in cyber defense exchange information and compile joint situation assessments. The second edition of the cyber security strategy was presented in 2016 and represents an interagency approach to all federal cyber activities. It identifies approximately 60 strategic goals and steps to improve cyber security in Germany.

For the first time, an attempt is being made to present Germany's security architecture as a whole. The framework for a sustainable and effective cyber security architecture is defined at the strategic level. The focus is on transparency among federal agencies concerned with countering cyber threats and on identifying fields of cooperation. Modern cyber security architecture is based on an understanding that the task involves a full-time effort. More than anything, it requires efficient coordination to make sure each agency knows exactly what is expected of it and to guarantee the smooth exchange of information.

Apart from the typical hacker attacks, the hybrid threats also include propaganda and disinformation. The intentional spreading of false information is used to influence the political discourse in other states, to build an atmosphere of insecurity and to destabilize societies. Since the Russian occupation of Crimea, attempts to influence public opinion have increased drastically. They are on the radio, on TV, and on social media networks, online newspapers and video platforms. For large parts of the population, the internet has replaced conventional media. This explains why the internet is the favored propaganda platform.

The aim of such campaigns is to create mistrust among Western states and within NATO. Every day a vast amount of unverified news is propagated on the internet, in particular via social networks such as Facebook. Moreover, it can be difficult to immediately tell the difference between meaningless chatter, substantially correct information and fake news. The rapid speed at which information is disseminated and the fact that people are inclined to believe what they read or hear present enormous dangers. Targeting specific audiences can manipulate public opinion or mobilize crowds, as was the case with a phony rape report in Germany. Certain media claimed that immigrants in Germany raped a German-Russian girl named Lisa. Many accepted this deliberate misrepresentation of facts as the truth, and demonstrations followed. In the end, the federal government had to step in to denounce the report.

A first attempt to counter such targeted disinformation was made two years ago with the establishment of the East StratCom Task Force, part of the EU's External Service Strategic Communications Division. The task force's working group on strategic communication in Eastern Partnership countries includes the states between the EU's eastern border and Russia's western border. Its task is to counter Russian disinformation in countries such as Ukraine, Georgia and Moldova, and to help shape public opinion. The task force publishes the weekly *Disinformation Review*, providing an overview of disinformation in the Russian media. The task force focuses on disinformation meant to cause unrest in the EU and cast doubt on mainstream politics, particularly in states with a significant Russian influence. They identify suspicious news for EU operations against disinformation, and report fake news to legitimate media outlets.

> ***It is only through strategic communication that public awareness of hybrid threats, and society's resilience against such manipulation, can be improved.***

Germany is setting up a network against hybrid threats that involves the Federal Chancellery, the Commissioner for Culture and the Media, as well as the Federal Press Office. The aim is to improve strategic communication, which plays a decisive role in countering hybrid threats. It is only through strategic communication that public awareness of hybrid threats, and society's resilience against such manipulation, can be improved.

However, building resilience against hybrid threats cannot be left to state agencies and institutions alone. A whole-of-society approach that includes civil society and the private sector is needed. The resilience of a society against hybrid threats largely depends on non-state actors. How companies protect their data and how private individuals handle information is not for the state to decide. That decision rests with the individual or the company. □

Winning the Information WAR

How states can marginalize hostile propaganda

By **Dr. Ieva Bērziņa**
Centre for Security and Strategic Research at the National Defence Academy of Latvia

PHOTOS BY THE ASSOCIATED PRESS

It's not easy to differentiate between propaganda and strategic communication. Both imply systematic and deliberate activities intended to influence the views, attitudes and behavior of target audiences in the interests of the communicator. Some argue that the essence of propaganda is in its manipulative nature. However, any communication that aims to serve certain interests is manipulative to some extent. Any professional communicator will inevitably highlight some aspects of a problem while toning down others, will construct messages by choosing the most appealing words and images, will calculate the most appropriate channels and intensity of delivering the messages, and will use the most authoritative opinion leaders to attain the desired result. All of these sophisticated activities are undertaken to influence public opinion, which is the aim of both propaganda and strategic communication.

Contrasting propaganda as false information versus strategic communication as truthful information is a misleading simplification because propaganda may be based on accurate information. The skillful manipulation of correct information often determines the propaganda's effectiveness. Propaganda has been described as an emotional type of communication that lacks rational arguments. However, this description relates primarily to human nature as opposed to the belief that propaganda is a wicked form of communication. Advertising models reveal consumer behavior is determined more by emotion than by rational thinking. This is even truer of political and military communication because it mostly covers subjects that audiences have not directly experienced. Thus, emotionality is also an inadequate differentiator because any communication must have emotional appeal to be effective. It would also be incorrect to label the information activities of non-Western international actors as propaganda — and those of Western countries as strategic communication — because the invasion of Iraq was the event that stimulated many Western academics to return to the concept of propaganda as a research subject.

Nevertheless, there is an important distinction between strategic communication and propaganda. The core idea of the strategic communication concept is to emphasize the word "strategy" rather than "communication." In other words, communication is a strategic function because every deed speaks more loudly than words. Thus, propaganda is distinguishable from strategic communication by its focus on purely communicative solutions, whereas the strength of strategic communication is in its interplay of policies and communication. Such a mindset encourages a focus on the actual needs and wants of audiences, which is a precondition for building strong relations between governments and societies. This is also a proper basis for resisting the influence of hostile foreign information because a strong society has greater immunity against information that is being used to damage its foundations. The collapse of the Soviet Union is a visible example because one of its main causes was a

False and misleading news reports are now a common tool of hostile propaganda campaigns. *PER CONCORDIAM* ILLUSTRATION

massive loss of belief in the system. There are four pillars for countering propaganda, based on this audience-centric approach: 1) measurement-based assessment of the influence of information, 2) comprehensive critical thinking, 3) strong civil society and 4) a positive vision.

The influence of information

The public opinion warfare that escalated in the context of the Ukrainian crisis and the emergence of ISIL/Daesh in 2014 marks an important milestone in the post-Cold War international system. Western countries that exercised global dominance after the dissolution of the bipolar world order gradually found themselves challenged in the information domain by non-Western international actors. This was largely possible because of the globalized information space, which enables worldwide information dissemination. Western audiences are now confronted with narrative battles and a clash of political communication cultures. For example, the lack of public demand for accurate information in authoritarian Russia allows a scale of manipulation that is difficult to understand in the West. As the boundaries between domestic and international communication become increasingly blurred, Russia is using the same approach in its communication with global audiences.

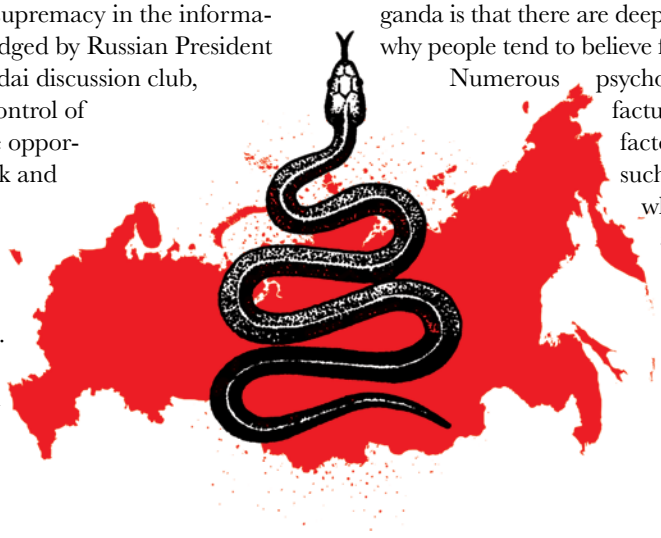
Such developments are disturbing in the West, to the extent that many prominent voices are claiming that the West is losing the information war against its opponents, mainly Russia. Interestingly, Russia also considers itself the loser in its information war with the West. For example, when Russia established information warfare troops, information warfare theorist Igor Panarin commented that Russia is much weaker than the West in this area and that it is losing because the West is forcing Russia to take a defensive stance and to make excuses. Western supremacy in the information domain was also acknowledged by Russian President Vladimir Putin at the 2014 Valdai discussion club, where he stated that the total control of global media gives the West the opportunity "to portray white as black and black as white."

Why are both sides of the information war presenting themselves as losers? There are at least two possible explanations. One is that the position of the loser in 21st-century information warfare provides a distraction from more important problems within society, mobilizes public support and increases funding for research projects, communication campaigns and the establishment of new institutions. This would be a purely propagandist approach. The other, more likely, explanation is that such statements are based on emotions, because there are no adequate metrics for measuring the influence of information. The West's perception of losing the information war seems to be based on the mere existence of Russia-promoted false or partly false media stories. But what is their actual impact on the total flow of information? To what extent have these stories influenced public opinion in Western societies? What is the causal link between public opinion in the West and Russia's information campaigns?

These are important questions because the target of information warfare is the cognitive dimension of society; media content is just a tool. Nevertheless, Russia's disinformation campaigns are now in the spotlight of many Western institutions and think tanks. Raising awareness of the strategy and tactics of opponents is an important precondition for resistance, but it is not exhaustive because opponents can be successful to the extent permitted by the vulnerabilities of the attacked side. It is also a matter of the allocation of intellectual and financial resources, because while focusing on opponents, the risk of losing domestic audiences exists, as revealed by a 2016 European Journalism Observatory study of Russian-speaking journalists in Latvia. One conclusion as to why it was difficult to develop pro-European media in the Russian language in Latvia was that all initiatives in this area were justified solely by the need to fight Russian propaganda, but that genuine communication with Russian audiences was not so important.

> ***The West's perception of losing the information war seems to be based on the mere existence of Russia-promoted false or partly false media stories.***

Another reason why prioritizing the debunking of disinformation is not the most effective way to counter propaganda is that there are deeper and more complicated reasons why people tend to believe false or distorted information. Numerous psychological studies demonstrate that factual accuracy is not the decisive factor in shaping people's views. One such study is social judgment theory, which explains that ideas will be accepted or rejected depending on existing beliefs and attitudes, rather than the truthfulness of the information. There are also many examples of purely false and fabricated media stories having very short life



cycles, while stories based on a context that supports the message are more effective. For example, an investigation by journalists with the online news site Meduza reveals one reason Russians in Germany believed the false story of a girl named Lisa being raped by immigrants was because the official handling and reporting of the New Year's Eve sexual assaults in Cologne decreased trust in the police. Therefore, it is impossible to plan effective measures against propaganda without a thorough understanding of why people think the way they do.

Critical thinking

The importance of critical thinking as an element for countering propaganda is determined in part by the peculiarities of the globalized information space and the specific rules of the game. During the Cold War, an "information iron curtain" separated the West and the Soviet bloc, which made it possible to operate relatively autonomously within each information domain. In the current circumstances, however, there is interaction between opponents. Thus, the Russian challenge in the information domain provokes reaction in the West, which leads to restrictions that may be interpreted as a limitation of democratic freedoms. For example, the ban on Russia's RTR-Planeta television channel in Lithuania in 2015 was presented by Russia's Foreign Ministry as "complete political censorship." Furthermore, the restriction of Russian media in the Baltic states was mentioned as an indicator of "the strengthening of totalitarian tendencies and manifestations of neo-Nazism in the politics of Latvia, Lithuania and Estonia" in a document adopted during the 2016 Regional Congress of Russia's compatriots from the Nordic states and the Baltic Sea.

It is profitable for Russia when democratic freedoms are restricted in the West because it provides Russia specific facts upon which to base its claim that Western countries are not democratic. Undermining Western democracy as a universal value is a long-term strategic goal for Russia because it aims to establish a polycentric world order with a diversity of political and economic models in contrast with the idea of a unipolar world order characterized by the global dominance of the West and the moral superiority of Western liberal democracy. If democracy fails in the West, the moral foundation for its global dominance is lost. Therefore, it is very important not to fall into Russia's trap through a well-intentioned desire to protect our own information space. Restrictive measures are not for open societies in a globalized information space.

The only reasonable way to protect the information space of democratic societies is to enhance resistance to hostile information in the cognitive dimension of society. When people are resistant to foreign propaganda, there is no need to impose restrictions on the free flow of information, unless it violates the law. The Latvian case provides evidence that such an approach works. Despite the fact that Russian television channels and other media are widely available in Latvia and the country has a large proportion of Russian speakers, trust in the Latvian media is almost two

Ricardas Savukynas, a business consultant and blogger in Lithuania, patrols social media to expose fake news attributed to Russian propaganda attacks on his country.

times greater than in the Russian media. Studies of human psychology confirm that, although it is difficult to change established views, it is possible to take preventive measures. The inoculation theory of communication states that an audience can be made resistant to hostile information by raising the threat awareness and activating arguments to strengthen existing beliefs. The International Research & Exchanges Board's (IREX) Learn to Discern program in Ukraine is a successful example of preparing society to resist the influence of false information. According to IREX data, training in media literacy skills led to a 20-plus percent increase in checking news sources, more confidence in analyzing news, and an ability to distinguish trustworthy news from false news.

Still, comprehensive critical thinking is very important in the sense that critical evaluation is applied not only to foreign information sources, but also to internal media. Most Western disinformation-debunking initiatives focus only on Russia. For the critical thinker that raises the question: Does the Western media always provide accurate and trustworthy information? This question needs answering because it would be wrong to expect people to apply critical thinking to information provided by non-Western actors, but simultaneously be uncritical toward Western media. A one-sided approach to disinformation and other types of media manipulation risks losing credibility. Furthermore, trust in the media is already decreasing in Western societies. According to a 2016 European Commission Eurobarometer survey on media pluralism and democracy, 44 percent of EU respondents disagreed that their national media provide trustworthy information. Gallup data show that trust in the U.S. media has dropped from 53 percent in 1997 to 32 percent in 2016. People in the West are critical toward their own media, and this should not be ignored. Perhaps a sound comparison with Russian media practices may improve the Western media's image. In any case, an open conversation about these problems could improve the situation.

Marchers with posters reading "PROPAGANDA KILLS" and "FIGHT" gather near the spot where Russian opposition leader Boris Nemtsov was gunned down near the Kremlin in 2015.

A strong civil society

A hallmark of current information warfare is the attempt by opponents to exploit the vulnerabilities in the relationship between state and societies in Western countries. Such strategies and tactics are enabled by the West's democratic freedoms and open societies. Russia's narratives about the immigration crisis in Europe are an example because they are gaining strength from a gap between popular opinions and government immigration policies. While political leaders publicly state that they welcome refugees, a Chatham House survey published in 2017 reveals that an average of 55 percent of respondents in 10 European countries believe that "all further immigration from mainly Muslim countries should be stopped." Russia gains an advantage when Western governments are unresponsive to the public mood. The Pew Research Center's spring 2016 Global Attitudes Survey shows greater confidence that "Vladimir Putin is doing the right thing regarding world affairs" among respondents in European countries with favorable views of far-right parties with strong anti-immigration views. During the 2016 Valdai Club discussion, Putin shared his views on this and other issues in Western countries and pointed out that the cause of the problem in the West is "that ordinary people, ordinary citizens do not trust the ruling class."

There is, indeed, a degree of truth in what Putin said. According to Standard Eurobarometer 86 data, trust in the EU decreased from 50 percent in 2004 to 36 percent in 2016; trust in national parliaments from 38 percent in 2004 to 32 percent in 2016; and trust in national governments from 34 percent in 2004 to 31 percent in 2016. Because this presents an opportunity for the purveyors of hostile foreign information, a dilemma arises as to what should be the priority — decreasing vulnerabilities or countering the opponent. There is a temptation to focus on the opponent because it is easier than addressing long-term systemic problems within our own societies. Nevertheless, many of the problems arise not from the influence of hostile foreign information, but from trends within Western societies. The "mediatization" of politics — meaning the political struggle takes place mainly in the media environment — is an important problem. Because the logic of the media business in free market economies is guided by the principle that "good news doesn't sell," the Western media tends to be overly negative, focusing on scandals and sensations, which is also a distortion of reality and truth. These trends in the information domain reinforce distrust in political institutions and lead to a decrease in political participation. Developing a genuine relationship between state and society can solve this and other problems.

The strength of civil societies determines the strength of democratic systems. Because elites are tempted to misuse political power, civil society must impose boundaries on the impunity of politicians. Thus, tension in society and state relations is an inherent feature of democratic systems, which should not be sacrificed as part of the information battle. Instead, developing new and better platforms for dialogue between governments and societies can increase mutual understanding and

accountability. Different forms of direct communication and solutions using new media technologies can be developed to circumvent traditional media. There is also a need for education and support programs for civic activism because political participation that allows for influence on political decisions is the only way to decrease alienation and improve the system. In other words, in healthy democratic systems, it is crucial to counter both foreign and domestic propaganda.

A positive vision

The final ingredient for countering propaganda is the formulation and communication of what we stand for and what we aim to achieve. In 2013, *Financial Times* columnist Gideon Rachman wrote the article, "The West is Losing Faith in Its Own Future." This is an accurate description of the problem in the information clash with opponents of the West. Russian Foreign Minister Sergey Lavrov wrote in a 2016 article: "There has been a relative reduction in the influence of the so-called 'historical West' that was used to seeing itself as the master of the human race's destinies for almost five centuries. The competition on the shaping of the world order in the 21st century has toughened." It is important to understand that there are two levels to Russia's challenge in the information dimension. One involves communication tools, including disinformation campaigns, which seem to be the main concern of Western communication experts. But the second, strategic level is a system of worldviews that represents a much more serious problem. It consists of many interwoven narratives: U.S. global leadership is worsening global security; the West is unable to manage the refugee crisis; Western democracy is dysfunctional; post-Cold War military interventions should not be permitted; and many others. The key problem is that many of the arguments used in Russia's narratives correspond, to some degree, to the views of audiences in the West.

Therefore, successfully countering propaganda demands a vision for future development that provides solutions to problems such as rising inequality, immigration, the environment, demographics, unemployment, radicalization and others. The promotion of a positive, inspiring and appealing future vision could distract attention from the opposition's activities and even make many of their arguments useless. For example, Russia's victory in World War II is a very important instrument in building its national identity and the consolidation of its compatriots abroad. The celebration of Victory Day takes place in Russia and abroad on May 9, which is also the date of Europe Day. Thus, instead of countering Victory Day, European countries, especially those with many Russian compatriots, could promote narratives about Europe Day as a positive and uniting alternative, which could also be used as a platform for debate about the future of Europe. Successfully countering propaganda requires not just refutation of opponents' arguments, but also proactive promotion of one's own perspective.

Conclusion

Structuring counterpropaganda measures around adequate situational awareness, enhanced critical thinking, a stronger civil society and promotion of a positive future vision enables the definition of a set of practical steps. A precondition for countering the influence of hostile information is the realistic assessment of its impact, which requires:

- A comprehensive system of monitoring and analysis of hostile activities in the information environment, including such domains as cyber, the media and social media.
- The operationalization of the concept of "resistance to the influence of hostile information in the cognitive dimension" by setting up metrics to measure the level of influence of hostile information and resistance to it within society.
- Research on the factors that determine a predisposition to be influenced by hostile information, which should translate into policies that aim to diminish vulnerabilities.
- Measurement and critical evaluation of the effectiveness of activities taken to counter foreign propaganda.

In the area of enhancing comprehensive critical thinking, the following would be necessary:

- Forecasting opponents' potential reaction to Western propaganda-countering initiatives and assessment of follow-on developments.
- Informing societies about opponent strategies and tactics, including in the information domain.
- Enhancing of media literacy skills within our societies, which includes critical evaluation of Western countries' domestic and global media practices.
- Improving the educational level of society.

A strong civil society as an element for countering propaganda can be attained by:

- Prioritizing issues of primary concern to society on the political agenda — unemployment, immigration, the economy, terrorism, etc., and effectively communicating policies developed in response to society's needs.
- Building trustworthy communication channels between governments and society, including the development of direct and dialogue-based communication practices.
- Enhancing political participation.
- Improving the quality of journalism.
- Acknowledging that reasoned criticism of governments is an indispensable element of democratic systems. Therefore, restrictions on civil society activism should not be imposed out of consideration for information warfare.

The promotion of a positive future vision requires:

- Defining measures for how better political, social and economic conditions will be achieved and translating these into an appealing and easy to understand future vision.
- Enhancing societal participation in the formulation of the future vision.
- Implementing strategic communication campaigns to mobilize and unite society around positive and inclusive events and an appealing future perspective. □

PROJECTING POWER

RUSSIA SEEKS TO RECAPTURE ITS IMPERIAL PAST BY EXPLOITING FORMER SOVIET COUNTRIES

BY DR. STEFAN MEISTER
GERMAN COUNCIL ON FOREIGN RELATIONS

PER CONCORDIAM ILLUSTRATION

Discussing Russia's attempts to influence former Soviet countries requires a thorough understanding of just how important the "near abroad" is to the self-understanding and legitimization of the ruling Russian elites. Those elites define Russia's role as a global power through its primacy as a regional power. As far as they are concerned, Russia can't be a global player without being the dominant power in the post-Soviet region. That mindset — along with Russia's nuclear arsenal and its seat on the United Nations Security Council — represents a potent Soviet legacy that defines Russia's self-perception today.

Russia sees its historical role in the region as justification for trying to influence the politics, economies and culture of former Soviet countries. Russian leadership regularly questions the sovereignty and borders of neighboring post-Soviet states, as Russian President Vladimir Putin did in August 2014 when he declared, "The Kazakhs never had any statehood." Or as James Sherr points out in his 2013 book, *Hard Diplomacy and Soft Coercion: Russia's Influence Abroad*, integration with the European Union is a "choice," while integration with Russia is "historically conditioned." Dominance over its neighbors is, to the self-understanding of the Russian elites, crucial to the survival of the Russian state. This mentality is rooted in Russia's history as an empire. Therefore, the Russian elites are willing to pay a much higher price to dominate the near abroad and prevent external players from questioning Russia's role than the EU and NATO are willing pay for rapprochement, support or the integration of these states.

This understanding also influences how Russian elites perceive change in the neighborhood. When political, social and economic change occurs through fundamental reforms — for instance, in the context of free trade and association agreements with the EU — it undermines Russia's political, social and economic hegemony and illustrates how political and economic reforms can bring post-Soviet countries closer to EU standards. The existence of an alternative to the Putin model is unacceptable to the current regime; Russia wants to set the rules and norms. Moscow tries to influence the region through informal relations and corruption. It prefers weak institutions and agreements based on personal ties. One reason Russia responded so aggressively to the Revolution of Dignity in Ukraine was to prevent the emergence of an alternative development model in the context of rapprochement with the EU. At the same time, Russia's military intervention in Ukraine represents a failed "carrot-and-stick" policy that revealed the limits of its soft power.

INSTRUMENTS OF INFLUENCE

Russia uses soft and hard power to influence its post-Soviet neighbors, though in reality the soft power is more like soft coercion. According to Sherr, soft coercion is "influence that is indirectly coercive, resting on covert methods (penetration, bribery, blackmail), and new forms of power, such as energy supply, which are difficult to define as hard or soft." On the soft side, there are carrots and sticks linked to economic and energy relations and a set of multilateral institutions dominated by Russia, as well as (mimicking Western policy) media and GONGOS (governmentally organized nongovernmental organizations) that try to influence the internal debate in these countries. On the hard side is a military buildup and the use of post-Soviet conflicts — or the creation of new conflicts such as the one in eastern Ukraine — to undermine sovereignty.

CARROTS AND STICKS

Traditionally, post-Soviet Russia has influenced its neighbors by controlling the supply of subsidized oil and gas. Price negotiations are an opportunity to remind these states of their dependence and limited sovereignty. At the same time, supplying oil and gas and creating intermediaries has presented opportunities for corrupt activities by Russian elites and the elites of neighboring states. Corruption and the possibility of self-enrichment are important tools of Russian influence and are a common part of the post-Soviet legacy. It creates loyalty inside Russia and in the neighborhood, and protects Russian interests in post-Soviet countries.

Russia also uses economic sanctions (such as restricting imports or increasing gas prices) to improve its bargaining position or prevent neighboring states from leaving its sphere of influence. The economic sanctions imposed against Ukraine the summer before the EU's November 2013 Eastern Partnership summit in Vilnius, Lithuania, are typical of how Russia applies pressure on post-Soviet elites at strategically important moments. For the first time, Russian leadership understood that free trade and association agreements between post-Soviet

A Russian warship in Sevastopol, Crimea, participates in the 2016 Defender of the Fatherland Day holiday, which celebrates the Red Army. When "soft power" efforts fail, Russia reverts to military might to influence former Soviet countries. REUTERS

states and the EU could undermine Russia's influence on its neighbors. In addition to the sanctions, or the stick, the Russians offered a carrot: a $15 billion credit to then-Ukrainian President Viktor Yanukovych to spare Ukraine from bankruptcy.

But Russian leadership always underestimates the role of societies in politics. The Russian elite's paranoia that the West creates the civil resistance movements described as "color revolutions" in post-Soviet countries is based on a belief that societies are passive and only motivated by leadership or external players. The Kremlin has been slow to recognize that societies are becoming more active in a globalized world — with social media a powerful tool of self-organization and communication. The failure to adapt to this changing dynamic is the source of Putin's repeated miscalculation of the social and political dynamics in Ukraine. Despite all the obstacles in the reform process, Ukraine has a vibrant civil society.

MULTILATERAL INSTITUTIONS

Multilateral institutions are an important way for Russia to connect with its post-Soviet neighbors. While the Commonwealth of Independent States (CIS) signaled the beginning of the end for the Soviet Union, it never succeeded as an instrument of integration. Institutions like the Collective Security Treaty Organization (CSTO), the security arm of the CIS, and the Eurasian Customs Union and later the Eurasian Economic Union (EEU) have been more successful at integration. The CSTO has become an important security tool in the post-Soviet region by allowing the Russian government to deploy troops in neighboring states or intervene in conflicts in a multilateral framework. There has been an agreement among CSTO members that rapid reaction forces can also be deployed in post-Soviet countries if there are domestic riots or color revolutions. The threat of color revolutions ties post-Soviet countries to Russia.

At the same time, membership in the CSTO gives access to Russian weapons at a discount, which is especially attractive to poor states like Armenia or Tajikistan. Being the dominant security actor and provider for post-Soviet countries is an important tool for Russia in terms of the dependency and vulnerability of its neighbors, especially in difficult economic times. Just before Armenia was to sign an association agreement and the Deep and Comprehensive Free Trade Agreement (DCFTA) with the EU, Russia questioned its continued military support of Armenia in its conflict with Azerbaijan over Nagorno-Karabakh. As a result, Armenia not only rejected the nearly finalized association agreement, but also joined the Russia-led EEU. Additionally, Russia is building alternatives to Western organizations, such as the Shanghai Cooperation Initiative, which helps to balance Russian-Chinese interests in Central Asia while strengthening ties with Peking on security and economic issues.

Russia, Kazakhstan and Belarus established the EEU in 2015. For the first time, Russian leadership tried to copy the EU and push economic integration among post-Soviet countries. It's a lesson Russia learned from the EU's successful economic integration efforts and a recognition that other post-Soviet integration projects have failed. The first EEU concept, presented by Putin in 2010, called for participating states to negotiate, under Russian leadership, a common economic space with the EU. However, since 2013-2014, amid increasing conflict with the West, the goal has been to prevent EEU states from integrating with the EU or at least to limit the access of other external players through increased trade barriers. Here, Russia again used a policy of carrots and sticks. While Armenia was threatened with a withdrawal of military support, Belarusian President Alexander Lukashenko negotiated a discount on oil and gas prices along with much-needed financial credit from Russia for joining. But those efforts can't overcome the main challenges to real integration in the EEU, which include Russia's dominance, the limited innovation potential of member states and the logic that authoritarian states will never give up sovereignty.

MANIPULATING THE PUBLIC

There is a growing significance placed on the direct and indirect manipulation of post-Soviet countries through Russian media, propaganda, disinformation and the Orthodox Church. Russian media has become a powerful tool, not only to influence public opinion inside Russia, but also in neighboring countries (and increasingly in the West). Because the Russian language remains the lingua franca in the region, a majority of Russian speakers, even in Baltic states, still watch Russian TV. Russian media has a huge influence on post-Soviet societies because it's often much better in terms of quality and entertainment than local TV. At the same time, it distributes an anti-United States, anti-NATO and anti-Western narrative. It often shows a world in crisis and the Russian president as the main stabilizing force for global peace. Russia as the island of stability and peace in a chaotic world is an important narrative. Russian TV and media have become powerful tools to reach out to the *Russkiy mir* — the Russian world — and create an alternative narrative to that of the Euro-Atlantic world. In failing to influence public discussion on the Beslan school terror attack, the Georgian conflict and the Sochi Olympic Games, Russian leadership has learned that it is crucial to dominate the information sphere at home and abroad. The Russian state has invested significantly in foreign media, but also in cyber attacks and in spreading negative and false narratives. Discrediting politicians, or the EU and U.S. policy media, has become a powerful tool for influencing societies in post-Soviet countries.

Furthermore, GONGOS and state-funded organizations, such as the Russkiy Mir Foundation and the Alexander Gorchakov Public Diplomacy Fund, are important instruments for reaching out to post-Soviet societies. Russia uses these institutions to influence public opinion and to create and distribute an alternative narrative to Western audiences, co-opted elites and stakeholders. The Russian federal agency Rossotrudnichestvo was established to increase ties with post-Soviet elites and societies and to coordinate policies and instruments to influence them.

The Russian Orthodox Church is another important element of influence. It plays a role as intermediator and influencer of societies in Russia and its neighborhood. It not only propagates the official Russian view of the world, but also anti-Western sentiments linked with conservative values and the independence of a traditional culture. The value discourse — which is linked to traditional views on family, anti-LGBT sentiments, anti-pluralism, anti-tolerance and to popular nostalgia — is well-received in the more conservative post-Soviet societies.

THE EU'S EASTERN PARTNERSHIP, CREATED TO STRENGTHEN RELATIONS WITH SIX OF ITS EASTERN NEIGHBORS (ARMENIA, AZERBAIJAN, BELARUS, GEORGIA, MOLDOVA, UKRAINE), SHOULD OFFER:

- A differentiation between those wanting political association, economic integration and maybe membership, and those only interested in cooperation.
- A focus on urgent needs. While European Union association and free trade agreements set long-term reform goals, short- and mid-term prioritization efforts are also needed.
- Improved security. Insecurity is a major challenge to sustaining reforms. The EU and NATO need to invest more in institution building in the security sphere, including border management training and addressing separatist conflicts. Eastern Partnership policy for transformation must be tied to other instruments of EU diplomacy and security policy.
- Strong institutions. Weak institutions represent a big challenge for Eastern European countries, especially when key institutions and authorities are controlled by vested interests that hold veto power over reforms. Institutions require external guarantees to ensure and enable their independence. New institutions are needed that allow the EU and its member states to participate directly with national and regional authorities in implementing reforms.
- Visa liberalization. Mobility is the single most important initiative the EU could take to signal to ordinary Eastern Europeans that deeper association with the EU can improve their lives.
- Support for participation in overlapping institutional frameworks for various policy areas, such as Moldova's and Ukraine's participation in the energy community or the Energy Union. The EU should allow associated partners to participate in mechanisms such as customs, border security and transportation policy, or in civil components of European security and defense policy.

Activists for nationalist groups mark Ukrainian Military Volunteer Day in Kyiv in March 2017 by blockading rail shipments that support Russia-backed separatists. REUTERS

HISTORY AND LEGITIMACY

History is increasingly becoming a key source of legitimacy for the Putin regime. The concept of Russkiy mir is a good example. Under that concept, all people who speak, feel and think Russian are Russians and have a right to be protected by the Russian state. That is a very fuzzy concept that not only includes ethnic Russians, but all people influenced by Russian culture and language, a huge number in the post-Soviet states where Russian culture and language were imposed by the Russian/Soviet empire. This Kremlin definition of the "responsibility to protect" is an important legitimization for intervening in neighboring states and for questioning their borders and sovereignty. Identity concepts such as *Novaya Rossiya* (New Russia), as some call southeast Ukraine, are based on a historic concept and are used to legitimize military aggression. At the same time, it justifies the concept of Ukraine as an integral part of a sphere of influence dominated by Russia. Domestically, Russkiy mir stands for external expansion and the ideology of victory, which helps to legitimize the regime in times of economic stagnation. Again, it is part of the great power projection.

HARD SECURITY

Lacking soft power and, increasingly, the economic resources needed to buy loyalty, Russia is increasingly relying on open and covert military attacks to prevent its neighbors from leaving its sphere of influence. The Russia-Georgia war in 2008 is an example. Russia used a military confrontation to de facto annex Georgia's separatist regions of Abkhazia and South Ossetia. From a Russian leadership perspective, this has prevented Georgia from joining NATO. In the Ukrainian conflict, Russia went even further and openly annexed Crimea through a referendum that did not meet any international standards, and then started a war in parts

of eastern Ukraine to prevent the country from further EU integration. This was at first a policy of weakness, necessitated by Russia's failure to bind Ukraine to Russia through a strategy of carrots and sticks. Only the covert military operation assured Russia's influence over Crimea (and Russian naval bases in Sevastopol) and over the post-Maidan Ukrainian government. But because of the muted reactions (no serious sanctions resulted from the war against Georgia) by the EU and the U.S., Russian leadership learned that covert military action and destabilization of a post-Soviet neighbor have only limited costs. These actions in Crimea had been prepared since the so-called Orange Revolution in 2004 and should not have surprised the West, nor Ukrainian leadership.

Managed destabilization — or "Bosnization" as some Russian experts call it in the context of the Ukrainian conflict — has become an instrument of Russian politics toward its neighbors. To create areas of lawlessness, corruption and despotism is an instrument of influence that prevents these countries from further integration with the EU or NATO. It also means that Russian leadership prefers unstable zones to a stable neighborhood. Supporting bad governance, in competition with EU-promoted good governance, has become part of Russia's policy in the neighborhood and is based on the limits of Russian resources. Destruction and destabilization are always cheaper and easier than stabilization and reconstruction.

Post-Soviet conflict zones often become areas of Russian influence outside of international law. These are more or less functioning entities, or pseudo-states, with administration and pseudo-elections, but without the rule of law and with despotism and limited or no access to the outside world. Sovereignty and borders are undermined, preventing integration with other institutions. Today, five of six Eastern Partnership countries have a protracted or separatist conflict in which Russia plays a role either as a conflict party or as the main negotiator. Moscow is either financing or subsidizing separatists, as in the cases of Abkhazia and South Ossetia in Georgia, Transnistria in Moldova, and Crimea and the Donbass in Ukraine. Simultaneously, in most of these conflicts, the Russian military is present in the separatist regions. Moscow is supplying the conflict parties with weapons, as in the case of Nagorno-Karabakh, and is the main ally of one of the conflict parties. These conflict zones are always a threat to their mother states because they give Russia the opportunity to intervene or challenge their security. The threat of destabilization and spillover of military confrontation and despotism is a constant threat. This, consequently, allows some post-Soviet regimes to legitimize autocratic policies.

WHY THE EU SHOULD DEVELOP STRATEGIC TRANS-ATLANTIC COMPLEMENTS:

- While only the EU can offer a conclusive framework anchoring Eastern European states, the U.S. can play complementary and supporting roles in the cooperation and security sectors.
- NATO can deepen its ties via practical means that can advance reforms while affirming open-door principles.
- EU reform and transformation offers can only be successful if linked to security guarantees, which at this time only NATO can provide. There is a need for more EU/U.S. engagement in the post-Soviet conflict zones.

WHY THE EU SHOULD ENGAGE ROBUSTLY WITHIN THE OSCE:

- In times of military tension, which increases the possibilities for accidents and misperceptions, the Organization for Security and Co-operation in Europe (OSCE) can provide a common platform for mediation, dialogue, trust building and conflict prevention.
- OSCE monitoring missions, such as those in Ukraine, bring transparency to conflicts and provide neutral information.
- Russia will perceive the OSCE as more relevant if Western countries invest more in the organization, take more ownership and raise their profiles. It is important to use this platform to address crucial security questions.
- Russia's control of the energy sector gives it influence over many European states and opens the door to corruption. Diversification, competition and interconnectors make EU members and their Eastern neighbors much less vulnerable to disruption and corruption.

A police officer stands guard near "green men" graffiti left by protesters on the side of a Russian Sberbank branch in Kyiv. The green men were camouflaged, pro-Russian gunmen who seized government buildings, banks and police stations in Crimea in 2014. AFP/GETTY IMAGES

DOMESTIC VULNERABILITIES

This policy of influence also succeeds because of domestic vulnerabilities in post-Soviet countries that are often weak and corrupt. Elites put their vested interests ahead of the country's future. Lack of reforms or rule of law, dominance of informal over formal institutions, and the disinterest of the elites in sustainable reforms make it easier for Russia to influence its neighbors. When there is no breakthrough in the reform process, vested interests are dominant and only small parts of society benefit from official policies. There can be no fundamental change. One strategy of post-Soviet states is to play both sides — the EU and Russia — to get as much personal benefit for the least possible reform. Lukashenko is a master at this game, as he is completely dependent on Russian credits and subsidies but at the same time periodically plays the card of a possible rapprochement with the EU.

There is a huge demand for security in post-Soviet societies. Insecurity, or uncertainty, is an important tool used by Russian leadership and post-Soviet elites. It's no surprise that security institutions in these states are often weak, underfunded and corrupt. They lack modern equipment, have limited deployment ability and are often linked with, or infiltrated by, Russian intelligence and security services. When Russia occupied Crimea with "little green men" — the name given to soldiers in unmarked uniforms — the Ukrainian Army did not react because it was ill-equipped and unable to respond to Russia's military dominance. In contrast, Russia began a fundamental reform of its army after the 2008 war with Georgia, upgrading its mobility, speed, communication and equipment. Russian leadership is now able and willing to respond militarily to any challenge in its neighborhood. The use of military power or show of force has become an important part of its policy in its near abroad.

Many elites in post-Soviet countries have no interest in good governance. They prefer informal rules and encourage corruption because it protects their power and rent-seeking opportunities. As long as civil society is weak, the internal pressure for change will be insufficient, and it will be difficult for outside reform forces to effect change. Elites in these countries have little interest in EU membership because the process of rapprochement and integration would threaten their authority. This is the case with the oligarch Vladimir Plahotniuc in Moldova, who owns Moldovan policy and has no interest in change. He and his political proxies constantly play the political game between Russia and the EU/West. Even in Ukraine, where the most developed civil society in a post-Soviet country outside of the Baltics is putting the ruling elites under pressure to reform the system, the resistance of oligarchs, such as Rinat Akhmetov and Ihor Kolomoysky, who benefit from the country's current state, remains a powerful force. Oligarch pressure has nearly stopped the reform process and weakened anti-corruption institutions.

This post-Soviet legacy makes all countries vulnerable to outside influences. It opens the door for Russian machinations to influence decision-making. The Putin regime has no interest in changing this legacy because it is a powerful tool of influence and prevents countries from adapting European norms and standards.

HOW TO RESPOND

It is crucial that the West does its homework. If the EU and U.S. fail to live up to their own standards and norms, they will fail to inspire reforms and development in Eastern Europe. If the EU and U.S. fail as role models, it will be easier for Russia to undermine the credibility of the West. If the Western democracies are not able to modernize and adapt to the changing global situation, it will be easier for autocracies to protect their model of governance. Russia's current political, economic and social model is unsustainable, but it will last longer if the West lacks responsible leadership and ownership of international crises. Russian leaders are willing to pay a high price to protect Russia's claimed sphere of influence, while European leaders appear unwilling to invest sufficiently in the stabilization of its eastern neighborhood. This short-term thinking can make the Russian president appear to be a powerful leader.

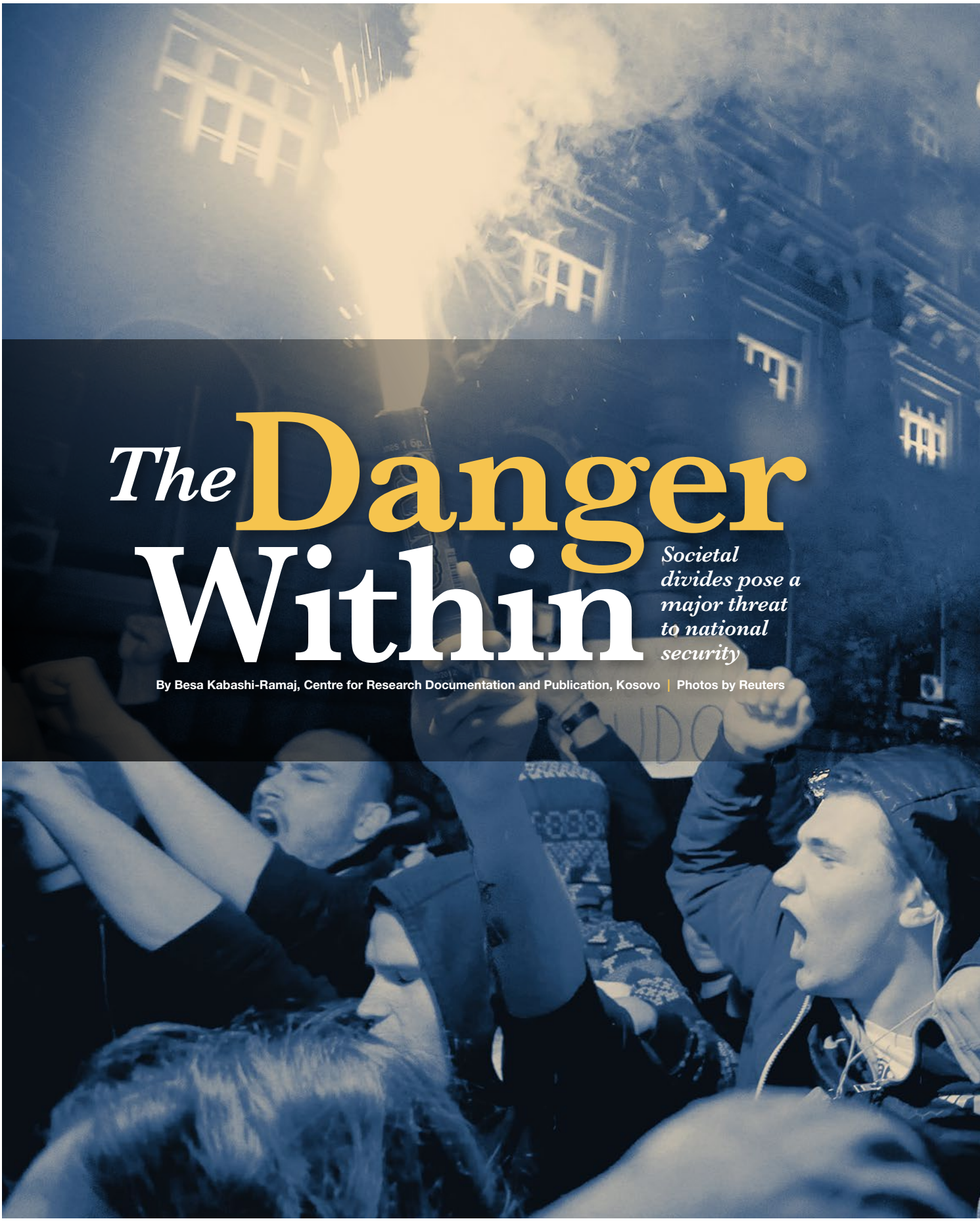
Resilience comes from within, through rule of law, good governance, a competitive media, checks and balances, transparency and functioning institutions. This is a generational task for all Eastern European countries. The West can help by serving as a role model and lending its expertise. The prospect of EU membership will not be a game changer for most post-Soviet countries. Many of their elites don't see a benefit in joining the EU, and many societies lack the understanding and the power to push for integration. At the same time, the EU alienates many of the countries that want to modernize by failing to offer a path to EU accession. Every European country that wants to join the EU should have the opportunity. But there should be a realistic assessment and communication on what it really means, how long it takes and how much it costs. There is a need for a selective integration model that is acceptable to EU members and interested countries. A multi-speed EU would offer new opportunities for partial integration for countries such as Ukraine and Georgia.

The EU should be more active in helping its Eastern neighbors with reforms. It should, when demanded by civil society and in places like Ukraine, offer expertise on reform processes and funding. There is a need to empower civil society and reform-oriented elites.

In most post-Soviet countries, internal weakness is as much a threat to peace, stability and development as external meddling. Russia is an aggressor and spoiler; these countries and their Western partners must prevent Russia from positioning itself as an alternative to real reforms. Sustained economic and democratic development throughout the region is a function of these states' capacity to provide security to their citizens and improve functioning institutions grounded in the rule of law.

Closer association with the West begins at home. Eastern European states should pursue democratic reforms not as a favor to the West, but as a benefit to themselves. Their societies and elites must decide if they truly want to reform and Europeanize by fighting corruption and building the rule of law and competitive economies, or if they prefer stagnation and weak governance. If these states fulfill certain conditions, the EU needs to ease visa restrictions to allow for freer movement between countries.

At this time, the EU's most important tools are association agreements and DCFTAs, which in effect bring the participating states closer to EU member standards. But it is important the EU not undermine its credibility by lowering standards in a rush to construct success stories. Less ambition, more adaptation to the realities of the participating states, and a tougher conditionality are important prerequisites for a successful change in these countries. □



The Danger Within

Societal divides pose a major threat to national security

By Besa Kabashi-Ramaj, Centre for Research Documentation and Publication, Kosovo | Photos by Reuters

Anti-government protesters rally in Belgrade, Serbia.

The global security framework and geopolitics have shifted since the Cold War and, as a result, so has the understanding of security. State security frameworks, once military-centric, now cater to societal and individual security concerns rather than the traditional Westphalian state concept, as noted by Alem Saleh in his 2010 article in *Geopolitics Quarterly*. In this new environment, security is no longer just about protecting states against foreign threats (national security), but also about protecting individuals (human security) and communities (societal security). While the concept of the state, and an understanding of the social contract, should mean that the population is secure in a secure state, this is not the case. In the last century, intrastate armed conflicts claimed more lives than interstate conflicts, according to the Human Security Report 2005. Threats to a country's national security are no longer dominated by conventional military threats, but have become increasingly complex and now include internal attacks on societies to destabilize states from within — a historically successful method often referred to as "divide and conquer." By targeting societal divides, states can be brought down from within without having to resort to open warfare.

In a globalized world, threats to the state include those aimed at its social cleavages and its people — threats meant to destabilize and undermine its sovereignty, sociologist Carlo Bordoni wrote in his 2013 article on the Social Europe website. The Westphalian system thrived during a time when nationalism was at the forefront of geopolitics, and on into the 19th and 20th centuries, when organizations like the European Union, NATO and the United Nations were created to pursue common security interests and facilitate peace. Nevertheless, Geoffrey Harris wrote in a 2015 paper for the EUSA Biennial Conference, at a time when security threats transcend traditional state borders, targeting societies and individuals, the state-centric perception of security is becoming less relevant. Terrorism is an example of a threat that cuts across borders but also feeds off societal cleavages at the expense of national security.

The modern state is in crisis due to a multitude of factors, including relatively recent historical and cultural changes, according to Bordoni. Economic and political choices affect societal security and the strength of the state, which may negatively affect people's everyday lives, widening already identified social cleavages and distancing the population from state institutions. States that do not deliver security feed even more societal disillusionment, instigating a crisis of state relevance. Consequently, Bordoni argues, state boundaries that once defined and united a nation and its traditions, culture, language, security and defense interests, become less defined, presenting a clear threat to the state as a whole. This highlights the evolution from conventional national security threats to a hybrid mix of threats that start with internal destabilization and end with the state at risk.

This shift in the international order in matters of security shows that "threats are more likely to originate from within, as opposed to between, states," as noted by James Bingham in a 2013 paper for King's College. In the current environment, a societal breakdown is a greater threat to national security than the threat posed by foreign forces. With globalization, the opening of borders, converging threats and risks, and a challenge to the general concept of the state, societal security — defined by Saleh as the ability to "sustain traditional patterns of language, culture, religion, national identity and customs" — is fundamental to national security. States that are able to foster strong and tight-knit societies are immune to negative influences and destabilization.

Tourists visit Taksim Square in Istanbul, Turkey. Economic and individual security affect a state's stability.

Despite this evolution in security threats, academia still focus predominantly on the traditional, dominant realist and neo-realist schools of thought, with the state as primary security agent. In this view, threats primarily relate to sovereignty and are of a military nature. Threats beyond this narrow view are considered irrelevant to national security, Paul Roe writes in his book, *Ethnic Violence and the Societal Security Dilemma*. In light of current events, it is safe to say that the realist and neo-realist views of security are far too narrow for present day challenges.

THREAT EVOLUTION

In contrast to the traditional international security framework, where threats to a state's security qualify as a security issue, the theoretical approach, as defined by the Copenhagen School, views threats identified as existential to the survival of an object as more relevant in today's international relations. The Copenhagen School's security-identity relationship has created a new way to look at security — as societal security.

French police gather outside a police station in Paris after a Molotov cocktail attack. Internal attacks cause people to question whether their state can protect them.

According to Roe, the Copenhagen School views Europe as a continent plagued by threats to group identity, ethnicity and religion, and by an overall lack of societal security.

The Aberystwyth School also contradicts the traditional and realist view of security, but differs from the Copenhagen School. According to the Aberystwyth School, genuine security can never be achieved through order and power, as the realists believe. Furthermore, according to the Human Security Centre, the state is viewed as a source of insecurity rather than security, considering that 90 percent of armed conflicts today are not between states, but within them. The Aberystwyth School teaches that security is achieved through the emancipation of people, rather than through the states. A commonality among people lacking security is the pursuit of basic needs such as food security, personal security, public safety and shelter. People who lack security also have common desires for more than just basic needs, according to Ali Diskaya in a paper for Aberystwyth University. These include freedom from fear and freedom to choose. In light of the hybrid threats to national security, security can be viewed as a combination of both the Copenhagen and Aberystwyth schools.

SOCIETAL SECURITY

A state's approach to societal security and its ability to preserve ethnic, cultural, religious and national identity is crucial to its security as a whole, assert Hynek Melichar and Markéta Žídková in their 2015 article for the European Consortium for Political Research. Failure to preserve identities can be viewed as a threat. If a state tries to deprive certain societies of their identity — through cultural cleansing or more drastic measures such as ethnic cleansing — defensive measures are adopted by the threatened society, ranging from nationalism to secession to violence. Identity-preserving countermeasures not only respond to the state's initial threat vertically, they also escalate horizontally by sparking reactions from other societal groups that perceive the first group's countermeasures as weakening their own identities. This escalatory process starts from a lack of societal security, and a misconceived state response ultimately leads to ethnic conflict and disintegration of the state, according to Melichar and Žídková.

Lack of societal security is a major disruptor of stability within a state

Lack of societal security is a major disruptor of stability within a state, but it also has tremendous implications for the state as a whole as exemplified by the former Yugoslavia and the Balkan wars of the 1990s. Roe points to Yugoslavia's

Demonstrators dressed as zombies in Kyiv, Ukraine, protest media that promotes subversive Russian propaganda. Disinformation divides societies and causes mistrust in the state.

disintegration as a textbook example of a country unraveling not because of external threats, but because of a lack of societal security internally. This entailed discrimination based on ethnicity and cultural and ethnic cleansing. The state's failure to provide for the preservation of all ethno-national groups' identities caused a defensive reaction, which initiated escalatory dynamics; an evolving nationalism that triggered others — including the state itself — to feel threatened, and ultimately resulted in ethnic conflict and the country's disintegration. Yugoslavia is a real-world example of the security dilemma. In trying to improve its security as a state, Roe explains, Yugoslavia further diminished the collective identity, widened already existing societal cleavages and decreased societal security, which in return initiated a vicious cycle that deteriorated the security of the state even further.

Before the current Ukrainian crisis, the concept of intrastate conflict within Europe was viewed with disbelief, especially given the EU and the promise of security and stability it represents. Russia's annexation of Crimea in 2014 and the subsequent insurgency in eastern Ukraine exposed the fragility of security, even within Europe. This may appear to be a conventional military threat by one state against another, but a closer look shows that the Crimea annexation resulted from internal societal divisions. Traditional realist and neo-realist views of national security, and threats to it, do not cover the complexity of the Crimean case. A closer look at the ethnic composition and history of Crimea, especially the history of the Tatars, shows that its vulnerability comes from within and is based on the historic challenges of meeting the security needs of different national and ethno-national groups. Melichar and Žídková argue that societal security equals sovereignty in importance to state security, considering the negative impact that failing to provide societal security has on a state's security and stability. It has also been argued that ethnicity and, primarily, a lack of economic security for the Russian population in Crimea, contributed to their role in the annexation. According to data collected in eastern Ukraine measuring the level of violence versus economic and ethnic activity, a lack of economic security played a bigger role in the conflict than identity (Russian language or ethnicity), Tymofiy Mylovanov reported in a May 2016 article for the website openDemocracy. A population that lacks societal security clearly becomes more vulnerable to foreign influences, perpetuating a violent cycle that starts with internal destabilization and ends with a serious threat to national security, constitutional order and even the country's continued existence.

ACCOUNTABILITY

State institutions and public appointees must improve accountability to their citizens. Bordoni argues that while the democratic system is supposed to ensure that citizens participate in decision-making, especially on crucial issues that affect their lives, the separation of power from politics creates opportunities for decision-making bodies to be nondemocratically appointed or controlled. Therefore, these powerful nondemocratic entities make decisions — pertaining to social, economic and other issues that affect masses of people — that fuse together a variety of political interests. People who are unable to change how these processes work and have to live with the consequences of such decision-making may suffer societal disillusionment and develop common cause with others beyond their state's borders, further weakening the state and its security, Bordoni writes. This inadvertently feeds further disillusionment with the state and its institutions and widens divisions within society, destroying a sense of national identity and making the society more vulnerable to external pressures and agendas that may target the state itself.

The traditional view of security is based on realism, with national security protected by military power. In fact, military power is seen as a crucial element of national security and sovereignty, as well as a political instrument to exert power, deter attacks, ensure domestic security, preserve peace and fulfill economic goals. While this argument is valid when discussing external threats to the state, military power has significant limitations when it comes to threats from within that are based on societal issues. Critics of the realist viewpoint argue that it serves only the elites and their interests at the expense of the masses. Defining national security only in relation to external threats and focusing on exerting military supremacy when threats increasingly come from internal societal discontent puts both the people and national security at greater risk. The post-Cold War era, nonetheless, has shifted from a more state-centric perception of security to a society-focused or individually-focused viewpoint, according to Saleh.

The rise of right-wing populism across Europe is a sign that societal discontent has increased and people are increasingly dismissing the traditional view of security, according to Harris. Another way to look at the phenomenon of increasing right-wing populism is to view it as exploitation of social discontent, a view argued in *Is Europe On the "Right" Path?: Right-wing Extremism and Right-wing Populism in Europe*, edited by Nora Langebacher and Britta Schellenberg. According to the book, right-wing populism is also a result of societal discontent and unequal distribution of access. Therefore, for states to respond adequately, their definitions of security must be broadened to include societal security. Additionally, their responses should be designed to counter contemporary hybrid measures that target internal weaknesses, especially societal divisions.

The evolution of the security concept coincides with a challenge to the function of states. If states are to improve societal security, their authority must be reinforced. This tests the realist view of security — centered on the interests of the state — and it may also pose a challenge to the core Westphalian concept of states. States, and the international organizations to which they belong, possess only as much power as that given by their constituents. If the function of states is questioned — as people broaden their view of what "security" and "interests" mean — the effects will be felt not just by the states, as they struggle to maintain legitimacy, but ultimately within international organizations such as the EU, NATO and the U.N. A decrease of functionality also decreases the legitimacy of states, which could harm their ability to sustain internal societal security, allowing for more fragile and failed states, Bingham notes. Again, Yugoslavia is a good example of this phenomenon; the main culprit of its internal armed conflicts and breakup was a lack of societal security and massive societal divisions. Markus Thiel argues in his paper, "Identity, Societal Security and Regional Integration in Europe," that the EU's slow integration process also contributes to the loss of functionality and to questions about the legitimacy of Balkan states that have failed to progress. In addition, according to Bingham, "The implications of fragile and failed states in a globalized world means that the consequences of state failure do not occur in a vacuum and can have security implications for the international community at large, not simply the populations of the states in question."

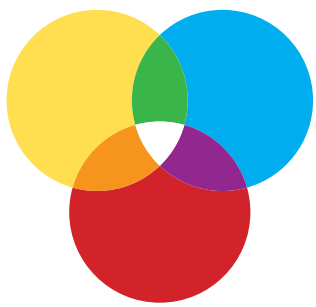
To persevere, states must be resilient and capable of adapting to new environments and accommodating geostrategic changes. This may mean that the entire concept of security has to be reviewed and redefined to reflect the world as it is today. This may also mean that the role of the state should be reviewed, as should the roles and missions of international organizations that were established under completely different circumstances. What is certainly clear, theoretically and in practice, is that national security is linked to societal security and, to preserve national security, states must safeguard the societal security of their populations. People should be provided the space and tools to preserve their ethnic, cultural, religious and national identities within the state.

CONCLUSION

Societal security has proven to be an important element of national security. Threats to national security have also become more sophisticated and complex, with internal societal divisions an attractive target for destabilizing a country. These changes have ramifications for all entities and agents involved in security and defense, including international organizations such as NATO. It is of vital importance to adopt a security concept that better fits the current global security environment and takes into consideration the complexity of new threats. This requires knitting together the traditional realist view of security with a contemporary broadened security concept that includes societal security. On a more practical level, Eastern European and Balkan countries must also adapt their security and defense efforts with greater understanding of the need for long-term national security solutions. Response and prevention measures should be designed to counter the threat shift toward the exploitation of internal societal cleavages to destabilize countries. But as a more effective, long-term solution, countries must also take measures to heal and prevent societal cleavages in the first place. As with health care, prevention is more effective and less costly than treating the disease.

In the case of the Balkan states, addressing the challenges each faces internally — such as institutional structural issues, rule of law, corruption and organized crime, but also inclusiveness and the sustainability of different languages, religions, ethnic identities and culture — is key to immunizing their societies against divisive, destabilizing measures. By addressing societal security, states would take more ownership of their citizens' well-being, creating more united and resilient societies, becoming more immune to external threats, creating a more self-sustainable security environment that is less dependent on international defense structures such as NATO, and ultimately increasing the functionality of the state in the international arena. Finally, as Tomas Jermalavičius and Merle Parmak write in their 2012 paper for Estonia's International Centre for Defence and Security, it is paramount that any state wanting to preserve national security, "preserve the cohesion of its society when it is confronted by external and internal stresses caused by socio-political change and/or violent disturbances." □

MANAGING DIVERSITY



The quest for ethnic and religious tolerance

By Andreja Durdan, Croatian Security Intelligence Agency

"No man is an island," wrote English Catholic cleric and poet John Donne in the 16th century. Today, this is more evident than ever. Nowadays we live in the age of identity politics. According to social identity theory, we are inclined to define ourselves by certain objective measures such as ethnicity, religion, race, gender and sexual orientation. These measures define our place in the community and society in general and are liberating and restraining at the same time. Socio-demographic changes and globalization are not optional, but rather the reality of our past, present and future. In the globalized world, states and societies face increasing permeability and fluidity, resulting in a challenging quest to manage diversity.

Multiethnic states are now the norm; the traditional nation-state (a distinct national group corresponding to a territorial unit) has become almost eradicated in the melting pot of today's world. Except for cases such as North Korea, it is now unrealistic to expect monoethnic countries and societies. An inability to reconcile the territorial integrity of the nation-state and a desire by minorities for cultural autonomy caused the failure of nation-states. If a nation-state doesn't recognize minority rights and attacks a minority's sense of distinct nationhood, it may increase the desire for secession and breed disloyalty. Globalization resulted in porosity of borders and improved technology transfer. It provoked, as the political scientist Michael Keating put it, "the three-directional erosion of the nation state" from above (by the rise of transnational institutions), from below (by demands of subgroups for control over some of the state's responsibilities), and laterally (the market erodes its permanency and superiority).

Despite the aforementioned, there are still attempts to impose monoculturalism in multiethnic environments at the expense of minorities, which often lead to intensification of minority efforts to protect and preserve their identity with a single goal — avoid marginalization. Assimilation on the one hand, and the urge for preservation of minority identity on

Protesters in the parliament building in Skopje, Macedonia, in April 2017 voice frustration over talks to form a new government. Turmoil in the country is rooted in ethnic tensions.
THE ASSOCIATED PRESS

the other, often cause intolerance, or worse — ethnic conflict. Would building a Pan-European identity be a silver bullet for ending ethnic tensions and discrimination, or are ethnically diverse societies the source of instability? Is the European "united in diversity" idea feasible in an era when globalization and migration have put a strain on European Union societies, causing collective fear after numerous terrorist attacks?

The course of the 20th century confirms that those who fail to learn from history are doomed to repeat it, as the philosopher George Santayana said. Because historical events have caused tectonic shifts that altered societies, new multiethnic societies have developed more integrative attitudes. Nevertheless, all EU member states face the challenges associated with capitalizing on that diversity and including all minorities in their societies. The inability to manage this emerging abundance of diversity is often rooted in ignorance and stereotypes, which result in defensive exclusion scenarios such as ultranationalism, the increase of right-wing radicalism, racism, shifts in populist policies concerning migrants and asylum seekers, re-animation of older conflicts in minority/majority relations, fundamentalism and anti-Semitism. This is reflected in anti-globalization and anti-EU feelings, as well as anti-Islamic propaganda. In these scenarios, state actors and the international community should act as arbiters and managers of diversity challenges. The quest for ethnic and religious tolerance is a precondition for the functioning of multiethnic states as predominant structures of globalized societies. For much of the 20th century, it seemed that religious tolerance and, up to a certain point, ethnic tolerance were prevalent in Western liberal democracies. However, recent events prove that much progress is needed to achieve harmony in ethnically and religiously diverse societies.

Diversity management is a voluntary organizational action designed to create greater inclusion in formal and informal social structures through deliberate policies and programs. Diversity management is also a prerequisite of a stable society. While like-minded groups may try to maintain equilibrium by banishing ideas and people they disagree with, diversity management helps to keep a social balance and harmonious coexistence. When ethnic groups feel disadvantaged, ethnic tensions and conflicts often follow. These conflicts are about more than ethnic differences. They are about territorial, political, social, cultural or economic issues that can result in the destabilization of states and whole regions. They are often accompanied by crimes against humanity, grave human rights violations, state failure and refugee flows. The role of external players can also deepen social cleavages. George Washington University Professor Michael Edward Brown underlined four levels of conflict triggers: internal mass-level factors (bad domestic problems), external mass-level factors (bad neighborhoods), external elite-level factors (bad neighbors) and internal elite-level factors (bad leaders). Neighbors and neighborhoods can cause cleavages when radicalized politics lead to diffusion, contagion and a spillover effect, or when governments decide to provoke conflicts in weak neighboring states for political, ideological, economic or security reasons. A successful management of diversity helps states and societies become less vulnerable to destabilizing threats from inside as well as from outside.

Tolerance

One key concept in diversity management is tolerance. The term connotes the acceptance of an action or a practice, or the foregoing of an opportunity to interfere in that activity or practice. It refers to a character trait or virtue of a person disposed to perform acts of toleration. These acts imply an intentional and principled decision to refrain from interfering when possessing the power to interfere. The latter is important to distinguish tolerance from resignation; hence it includes aspects of voluntarism. Its intention is to ensure both the individual's right to autonomy and individuality as well as social progress and democratic governance. The paradox of tolerance, as many philosophers have stated, is presented through the concept of objection as a precondition for tolerance — meaning tolerance is required only for the intolerable. Which raises the question: Why tolerate something we consider to be wrong?

There are many types of tolerance and, accordingly, many types of intolerance. Tolerance can be political and social. Political tolerance is an important democratic value because it refers to the willingness to extend

A billboard advertises an Anne Frank exhibition in Šibenik, Croatia, in February 2017. Religious tolerance is critical to fostering peaceful societies.
REUTERS

civil liberties to groups considered objectionable. Social tolerance involves lack of prejudice, rather than one's ability to overcome such prejudice. Prejudice is a negative intergroup attitude based on false, simplified or overgeneralized beliefs. As Bruce Hunsberger wrote in his 1995 article, "Religion and Prejudice: The Role of Religious Fundamentalism, Quest, and Right-Wing Authoritarianism," prejudice consists of three components: a cognitive one (involving a set of beliefs or stereotypes about a derogated out-group), an affective component (entailing disgust or visceral dislike for the out-group) and a disposition to behave in a socially aversive way toward members of the out-group.

These types of tolerance tend to occur more often in societies and political systems where exposure to diversity is emphasized. There seems to be a positive correlation between tolerance and exposure to diversity (racial, ethnic, religious), while diversity tends to provide an incentive to lessen the reliance on established beliefs and predispositions. To underpin this argument, some researchers, such as University of Quebec at Montreal Associate Professor Allison Harell, have shown that exposure to ethnocultural and other diversity decreases prejudice among social groups, primarily due to identification with out-group members. Racial and ethnic diversity may decrease tolerance for intolerance by fostering identification with the minorities at which intolerance is aimed. This kind of diversity may also foster cognitive skills that increase tolerance for objectionable groups, a phenomenon demonstrated by the fact that people living in diverse networks tend to exhibit multicultural tolerance.

Exclusionary intolerance is enhanced when a group interested in reinforcing its distinctiveness wants society to respect its right to be intolerant of other groups. On the other hand, inclusionary intolerance arises when minority groups are trying to fully participate in society (e.g., preferential hiring regulations). As for ethnic intolerance, it can refer to ethnic hatred, ethnic conflict, discrimination, racism and ethnic nationalism. These deviant forms, if tolerated by the state, lead to demonization of minorities and, as recently seen in Europe, the rise of nationalism, wider enthusiasm for racist, xenophobic, anti-Semitic, anti-migrant and anti-refugee rhetoric and attitudes. Europe is currently in a paradox. It is experiencing its greatest diversity ever — a result of greater mobility, more contact and intermarriage. Yet, simultaneously, there is an increase in the number of people who find this diversity to be a problem. They believe the chance for democratic progress and prosperity is greatly reduced when minority concerns are given acknowledgment and affirmation. A deep polarization in European society is occurring, requiring an immediate and comprehensive reaction and approach.

What can be done to promote tolerance and concurrently breed further diversity in modern liberal states? To this end, good governance based on a functioning rule of law is crucial. It plays a vital role in including minorities in societies and protecting their rights and interests through dialogue and recognition of problems. Political representatives and community leaders play an important role, as do the media and educational institutions. In this respect, social networks tend to be significant factors, especially for the younger population. Legislative measures should criminalize different forms of intolerance and institute tougher penalties for violators. Monitoring minority employment should be enhanced in areas where they are underrepresented. Forming advisory bodies that include minority representatives should be considered. Raising public awareness through the media and government campaigns and establishing institutions to monitor and prevent discrimination should be a priority. Promoting the empowerment of minority rights through education and ensuring adequate national and local social networks should be encouraged.

Exclusionary intolerance is enhanced when a group interested in reinforcing its distinctiveness **wants society to respect its right to be intolerant of other groups.**

As for a comprehensive approach, the international community should be involved, provided the intervention occurs in due course. To avoid ethnic conflict and wars, it is essential to avoid repeating historical scenarios seen so many times in different areas of Africa, Europe and Eurasia. The role of external powers in ethnic conflicts is indisputable and can be manifested through conflict pacification mechanisms and democratic consolidation mechanisms, reconciliation and economic recovery. Traditional peacekeeping is obviously insufficient, and a new approach is required to maintain international stability and prevent spillover effects in unstable areas and fragile states. International efforts should be initiated by the United Nations at a global level, by relevant bodies at a regional level (the EU, the Council of Europe and the Organization for Security and Co-operation in Europe), and by all other actors included in peace building, peacekeeping and international cooperation. Syria, most recently, and the Western Balkans only a few years ago are good examples of failed preventive diplomacy and late international engagement. The late international community response caused things to move in an unwanted direction — the emergence of terrorist and radical groups, migration waves, demographic shifts, unstable and unsustainable political systems, and instrumentalization of conflicts by superpowers.

The goal of minority integration policies should be to foster long-term stability, rather than the belligerents merely appeasing the international community while monitored by international actors. The most prominent example is Bosnia and Herzegovina (BiH). The way the coexistence of BiH's three main entities works — or rather does not work — is the

Kosovo Serbs watch in January 2017 as bulldozers tear down a concrete wall in Mitrovica that raised tensions between Kosovo and neighboring Serbia. The removal followed an agreement between the government and the ethnic Serb minority.
THE ASSOCIATED PRESS

cause of constant clashes and instability. BiH is a state of great differences that lacks unity and where exceptions are rules. As the novelist Ivo Andrić stated: Where logic ends, Bosnia begins. With its three states within a state (Federation of BiH, Republic of Srpska, Brčko District), BiH is haunted by recent war traumas and numerous diverging interests, while yesterday's victims and assailants must coexist in coercive conviviality.

Integration failure leads to fragile states, with societal and institutional dynamics being the main drivers of that fragility. These fundamental dynamics frame how more formal institutions and processes work and thus determine the quality of government and the inclusiveness of the economic and political systems. Fragility is a (dys)function of social cohesion and institutionalization. Combined, they determine the capacity of a population to cooperate and to direct this cooperation toward national-level challenges. Fragile states, if left in status quo, tend to collapse.

Southeast Europe/Western Balkans

One of the most prominent examples of the aforementioned diversity is the Western Balkans region in Southeast Europe. History defines the Balkans as a political region. A peripheral European location, divergent population distribution and historical migrations concurrent to emerging new states affected the region's formation and ethnic and religious structure. Several ethnic areas were formed based on their spatial identity (Christian culture) and dominant language (Slavic, Latin and Greek). Efforts to establish autonomous national identities or rigid concepts of autonomous states, cultures or geographic space often resulted in conflicts (the Albanian movement, Kosovo independence, the war in BiH) and evident intolerance for diversity, especially ethnic and religious. Throughout the 19th and 20th centuries, this area became ethnically and religiously diverse, making the situation even more complex. The lack of stability caused the development of geographically-shifting states, migration of endangered populations and socio-demographic changes.

As a reflection of this diversity, there are Albanian, Bulgarian, Bosnian, Roma, Greek, Croatian, Macedonian, Hungarian, German, Italian, Russian, Ukrainian, Ruthenian, Romanian, Serbian, Montenegrin, Slovak, Czech, Slovenian, Turkish, Tatar, Gagauzian and Jewish minorities living in Western Balkan countries. A nationality may be a disadvantaged minority in one state while forming the majority in a neighboring country. The movement to absorb Kosovo into a new Albanian majority state in conflict with Serbian interests — along with the Macedonian-Greek dispute and the inability of entities in BiH to coexist — could lead once again to severe fragility across the region. Because of conflicts, these struggles are associated with minority issues and a reluctance to embrace diversity as an asset rather than an obstacle. The author Andrew Heywood defines the term "balkanization" in political science as fragmentation of a political unit into antagonistic entities. This term defines the Western Balkans.

As far as religion is concerned, religious participation plays a major role in the identification of communities. Christianity (Catholics and Orthodox) and Islam are the predominant religions in the Western Balkans. Historically, Turkish influence since the Ottoman Empire made the spread of Islam in this area an important factor in creating ethnic identity and restructuring, especially in BiH. In certain parts of BiH or Sandžak, religion has become symbolic of spatial reservation, which leads to further homogenization and segregation. Religious intolerance is becoming more blatant and raising alarms in certain areas. It is fueled by poor social, economic and educational standards, such as in Sandžak, where 70,000 Muslim Bosnians are the largest minority. It leads to ghettoization, redefinition of ethnic lines and further conflicts. Concurrently, it leads to an increase of orthodoxy and religious fundamentalism, radicalism and extremism, often encouraging terrorism and giving rise to the foreign fighters' phenomena. The spread of radical religious ideas led not only to intolerance, but to micromigrations of people leaving areas under rigid religious laws and causing further homogenization

of religious entities. Furthermore, religious identity in these situations is strongly connected to national identity. In areas where there are two or more conflicted religious communities, religion tends to take over the role of cultural protector. Hence, religious identities become their way of expressing and emphasizing ethnic identity.

In the post-conflict countries of the Western Balkans, diverging war memories and experiences, trauma and economic weakness threaten regional stability. Although efforts are made to overcome ethnocentrism and religious homogenization, it seems the instrumentalization of differences overrules the reconciliation process. In addition to bilateral and regional issues, most Western Balkan countries have Euro-Atlantic integration aspirations, and some must contend with (not so) latent Russian influence. Given the historical and socio-economic context and unequal policies, managing diversity poses a great challenge for regional governments. It is indisputable that societal and political transformation have gained ground in the Western Balkans and that people must learn to live with diversity and perceive it not as a threat to their identity, but as a catalyst for their progress and development. Excessive adherence to all aspects of the nation-state in this era of globalization means disregarding international cooperation and reversing progress toward regional cooperation and coexistence. Western Balkans countries, such as Croatia, with more experience fostering democratic equilibrium and economic stability, are working to develop and manage diversity — ethnic, religious, cultural and otherwise.

Croatia

The treatment of minorities in the Western Balkans and the rights and accommodations accorded to them vary by state. Croatia is an EU member and a multicultural state. Its multicultural structure is visible in the relationship between the Croatian majority (90 percent of the population) and the 22 officially recognized minority groups geographically dispersed across the country. The largest minority is Serbian, represented by 4.3 percent of the population. Regarding religion, Catholics are dominant (86 percent) followed by Orthodox Christians (4.4 percent). The dominant language is Croatian (96 percent).

To some extent, Croatia is still experiencing the adverse effects of systemic transition and is dealing with minority issues in the context of relations with neighbors burdened by the war in the 1990s. This effect is especially present near the borders. Croatian multiculturalism is primarily based on cultural diversity among minorities. Migration flows haven't really affected the Croatian demographic structure yet, since Croatian immigrants are mostly Croats previously living in other Southeast European countries. But what might be concerning is the recent economic emigration out of Croatia.

Croatia has established a solid legal framework for dealing with minority issues — full expression of minority identities is protected through constitutional provisions, laws and adopted international legislation supported by media pluralism and state and local policies. Croatia's legislation is fully harmonized with European values and standards and derived from key international legal instruments dealing with human rights. The Croatian Constitution, as a paramount legal act, guarantees rights and freedom for all, regardless of ethnic or religious origin. It ensures free expression of national/ethnic/religious identity, use of their language and writing, as well as cultural and educational autonomy. Also, minorities are represented in the parliament (eight representatives) and at the local level (councils of national minorities and individual representatives). Preferential hiring regulations for minorities are applied. To help further diversity, two state organizations are in charge of minority issues — the Council for National Minorities and the Government Office for Human Rights and the Rights of National Minorities. Minority organizations are numerous, especially in the media and culture. Government and local administrations are investing in media campaigns, workshops and campaigns aimed at raising awareness.

In general, Croatia's minority communities appear well integrated into Croatian society, especially the Muslin community. The Roma community is making noteworthy progress in its assimilation. Still, Croatia is not a country with a perfect minority record. The recent war has put a strain on the perception of certain nationalities, especially the Serbs, who are the largest minority. Returnees and communities on the Serbian border often fail to assimilate, invoking past conflicts and misusing their lawfully granted rights for personal gain. In addition, some minority organizations and nongovernmental organizations are perceived as existing primarily to siphon state financial support. Another issue is the instrumentalization of minorities for political purposes by their home countries.

Misusing ethnicity

Ethnomobilization, according to the authors Antonija Petričušić and Mitia Žagar, is the instrumentalization of ethnic identities — the misuse of ethnicity by elites to mobilize the masses for the realization of their political (and even personal) objectives and interests. The most prominent example in the Western Balkans is the era of Slobodan Milošević, former Yugoslav and Serbian president. After the dissolution of the Socialist Federal Republic of Yugoslavia, the grouping along ethnic lines and re-emergence of ethnic cleavages resulted in social segmentation. Many politicians of the Serbian establishment manipulated public opinion by employing distorted pre-existing narratives and myths, rearranging historical facts and intentionally fostering insecurity and fear. Milošević mobilized the masses to legitimize his rise to power, install allies in Montenegro and deny autonomy to the provinces of Vojvodina and Kosovo. Instrumentalization of ethnic media (to serve the interests of stakeholders rather than the public) was used to generate intolerance. Milošević's establishment used the Orthodox Church to spread the idea of a "greater Serbian statehood" and intolerance toward all who didn't want to live in that nation. The education

During a day of remembrance in April 2017, relatives visit the graves of family members killed by Serb forces near Gjakova, Kosovo, during the war between ethnic Albanian rebels and Serb forces.
THE ASSOCIATED PRESS

system was used to spread official political propaganda and to control the thinking of future generations. Politically reliable faculty made sure that ethnic or religious diversity was reported and punished.

In the deeply divided societies of the former Yugoslav republics, different issues occurred based on religious and ethnic origin. The role of religion in the Balkan wars was evident but not in the forefront. Conflicts were nationalist-based. Symbols of Croatian ethnic and religious presence were destroyed in predominantly Serb-populated areas to rewrite history and claim it belonged to the Serbian majority. Milošević's propaganda was stark and comprehensive, intended to spread radical nationalist ideas and the separatist claims of Serbs in Croatia. Even after the international community became involved, it took a long time to achieve relative stability in the Western Balkans. The international community's efforts to perpetuate existing regimes, rather than facilitate transition and transformation, prolonged the conflicts and proved that no state can survive without the support of its citizenry, which in this case consisted of multiple ethnic and religious groups.

Even today, attempts by radical actors to instrumentalize minorities, the media and the religious establishment can incite general intolerance and bad relations. Although there has been significant improvement in minority policies (mostly due to conditions imposed by international organizations), minority issues still pose a great stumbling block in bilateral and multilateral relations of former Yugoslav countries. Without the ability to learn from history and use it to manage diversity, the region will be doomed to repeat history.

Conclusion

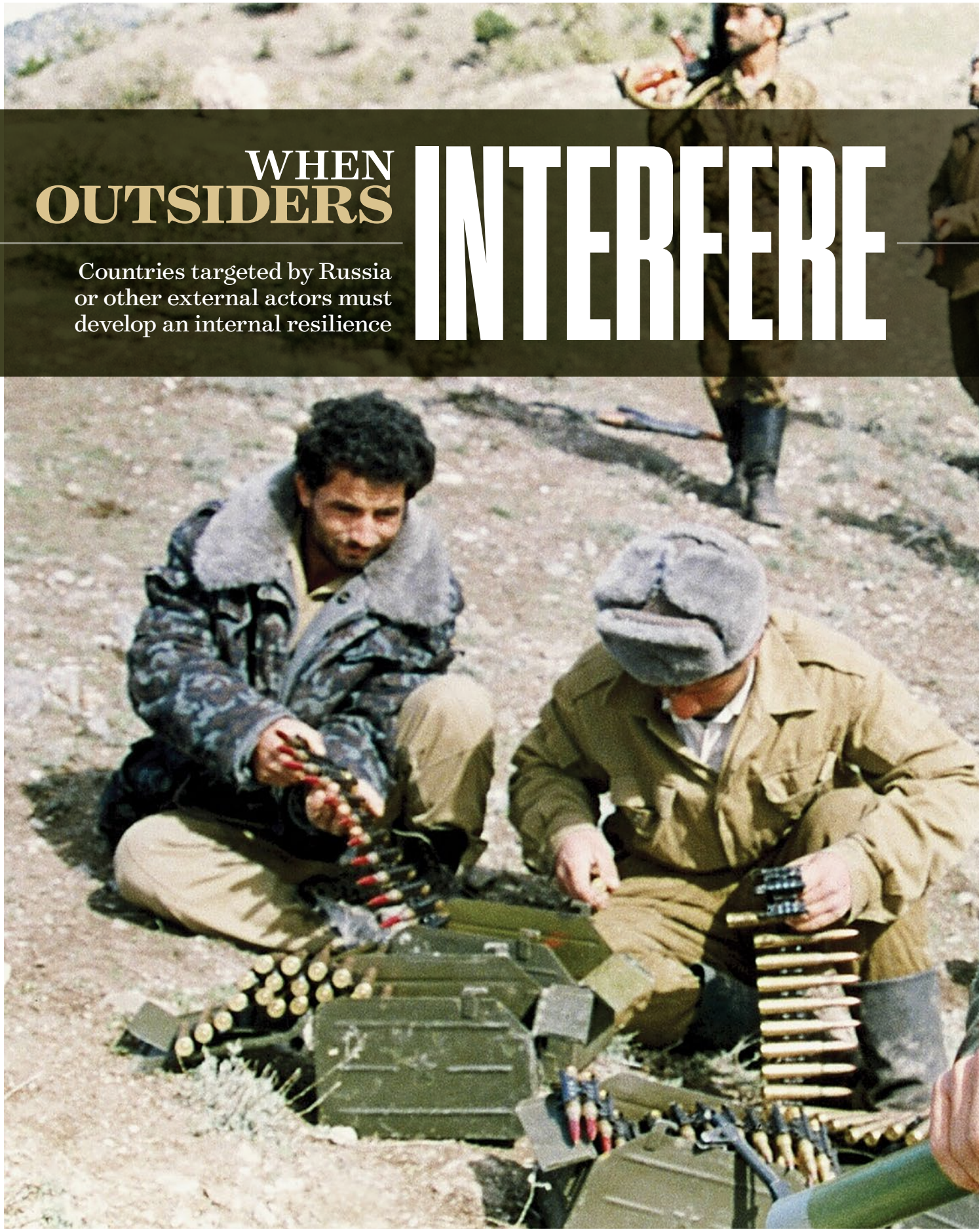
It is undeniable that people in advanced democracies will become more diverse. But diversity management can only succeed with a determined effort at the international, local, political and social levels. The quest for ethnic and religious tolerance emerges from historical and social changes that pave the way for diversity. Managing this diversity has proven difficult even for established democracies.

Tolerance should be proactive, engaging and comprehensive in a way that involves all state and nonstate actors, members of the community and minorities. States should have a functioning system based on solid and consistent legislation. Local communities should engage in different projects and programs to include minorities in all aspects of life. Political tolerance alone is not adequate; it should be accompanied by social tolerance, which is crucial for integration. As far as religion is concerned, states should refrain from interfering in religious practice and act as a neutral arbiter between competing groups within society. The state should prevent attempts by any group to interfere with the practices of others. Inadequate social integration and a lack of tolerance leads to segregation, imbalance and serious complications.

As contemporary democracies become more diverse ethnically, racially and linguistically, serious questions must be answered about the balance between social equality and individual liberties among marginalized groups. Tolerance should be used to ensure both individual rights to autonomy and individuality, as well as the larger goals of social progress and democratic government. Strong and inclusive societies are less prone to destabilization. □

WHEN OUTSIDERS INTERFERE

Countries targeted by Russia or other external actors must develop an internal resilience



By
Pál Dunay, Ph.D.
Marshall Center

Azeri soldiers prepare to fight ethnic Armenian separatists in the breakaway region of Nagorno-Karabakh in October 1992.
AFP/GETTY IMAGES

The post-World War II era has been one of increasing international cooperation and the empowerment of multinational institutions. But the Euro-Atlantic area is facing a new division. Some states would like to return to the Westphalian international order and its inherent strong state sovereignty in the hope of avoiding international interference in their internal affairs. For the Russian Federation, this concept is the foundation of its foreign policy and, as pronounced by Foreign Minister Sergey Lavrov on numerous occasions, Russia believes a majority of states share this view.

Certainly, this view appeals to leaders who seize power and do their utmost to perpetuate that power. However, it is doubtful most of Europe agrees. Many Europeans live in a post-Westphalian world where states, societies and people interact freely, human rights matter more than state sovereignty and globalization, in spite of its downsides, is regarded as advantageous — an engine that creates more affluence for everybody. Nevertheless, a state's behavior rarely follows neat theoretical constructs. States that tout noninterference often claim the right to interfere in the affairs of others, and even liberal countries occasionally object to having the same standards apply to them that they apply to others. Still, there are limits to relativity; it is nearly universally acknowledged that living in Sweden or Germany is better than living in North Korea or Somalia.

States use various justifications for interfering, often pointing to values and interests, historical and ethnic links, or anything else they see fit. On a more concrete level, states use various grievances, such as discrimination against, or mistreatment of, minorities (or in extreme cases, genocide) to legitimize interference. Those who view international relations through the lens of international law should be aware that many instances of interference are within the rules. States have an elementary interest in influencing their environment favorably. However, the fact some interactions are legal does not mean they are welcome, and legal equality is distinct from military or economic equality. Thus, states and societies must develop a capacity to resist and react to challenges in order to restore equilibrium. Call this "resilience." In extreme situations, resilience is how states and societies resist collapse under the weight of disastrous events.

Resilience is only possible if the state and society anticipate the potential consequences of events, be they man-made, caused by natural disaster, or the result of internal or external challenges. Consequently, resilience is contextual; its many forms are dependent on the environment. It is also contextual in the sense that each state and society prioritizes the threats and challenges against which it develops resilience. Resilience incorporates governance, the cohesion and support of society and state capacity, which can be developed with the help of internal and external forces.

Protracted conflicts

The area of the former Soviet Union — a strange term to describe a group of countries 25 years after the Soviet state dissolved — has the characteristic features of a regional security complex; its security relationships can be interpreted only in connection with each other. However, it stops short of being a security community, characterized by intense cooperation among the parties and a prohibition on war against each other. It is worth noting that these countries, long part of the same country, cannot always establish harmonious relationships today. Fortunately, the dissolution of the Soviet Union was largely peaceful, though violent conflicts erupted in its final years and, more recently, after its demise.

The term protracted conflicts refers to those in a lasting stalemate with little promise of resolution. Introduced in the post-Soviet era, the concept addressed a number of conflicts in the south Caucasus and one in Moldova. None of those conflicts has been resolved, and new ones have emerged. The term is arbitrary in two senses: The geographical scope of its application is confined to the west and southwest of the post-Soviet space (excluding other conflicts of lower intensity, such as in Central Asia), and the conflicts to which the term refers are in different phases of the conflict management cycle.

In 2014, two conflicts broke out within Ukraine's borders — with the significant involvement of Russia, including its armed forces — after mass demonstrations against the political course set by Ukraine's pro-Russian president, Viktor Yanukovych, resulted in his ouster. Other conflicts, such as those in Abkhazia, South Ossetia and Crimea, have been terminated but not resolved. This is negative peace without positive peace. Still others, such as the Nagorno-Karabakh conflict, threaten to return to high-intensity violence.

It is open to question which divisions or social cleavages are at the root of these conflicts and what contributes to their perpetuation, meaning there is a need for sober analysis on how to overcome these divisions. Although the protracted and potentially protracted conflicts do not have identical roots, a few common characteristics can be identified:

- Most protracted conflicts date to the decline of the Soviet Union in the late 1980s/early 1990s. The oppressive Soviet central apparatus weakened significantly, allowing a freer expression of disagreements in some societies and caused the unified "Soviet people," which turned out to be little more than a popular illusion, to splinter into groups formed from the Soviet Union's constituent nationalities. Hence, long-suppressed ethno-national animosities resurfaced.
- Questions also arose regarding territorial arrangements that the Soviet leadership once regarded as insignificant. The nearly bloodless dissolution of the Soviet Union in accordance with the *uti possidetis* principle was a great achievement. However, it gave way to some centripetal tendencies that drove smaller entities toward *de facto* autonomy, or even attempts at *de jure* separation. Russia was not immune, either, though central power was sufficiently strong, and a determined use of force against Chechen separatists maintained its territorial integrity. Other less determined, less powerful states have been less able to rebuff separatism. Russia capitalized on this weakness by forcibly annexing Crimea from Ukraine.

- Often, these conflicts had an ethnic basis. It is clear that the Abkhaz did not feel accommodated in Georgia, something they made clear even while Georgia was still part of the Soviet Union. And South Ossetians understandably felt closer to their ethnic brethren across the border in Russia's Republic of North Ossetia-Alania than to Georgians. The Transnistria-Moldova conflict is somewhat similar, because the ethnic mix in Transnistria is different from that in the rest of Moldova. This dates to the historical reasons that Moldova's (and the Soviet Socialist Republic of Moldova's) current state borders are not identical to the historical borders that predated World War II. Last, but not least, the Nagorno-Karabakh conflict revolves around a combination of territorial and ethnic issues.
- Those factors do not offer a full explanation of every protracted conflict, because other factors may have complementary roles. Economic factors, including the level of development and trade patterns, play a role, as is clearly the case in both Transnistria and Ukraine's Donbas (Donetsk and Luhansk). Both areas are more industrialized and have traditionally generated a higher per capita gross domestic product (GDP) than the national average. Their economies are linked far more to Russia than to the rest of the countries to which they belong. Before the conflict broke out in 2014, 70 percent of the Donbas' external trade was with Russia, and the share (if not the volume) has since increased. Hence, people there are understandably supportive of building connections with the main economic partner. Russia may be a relatively small player in the world economy, representing less than 2 percent of the world's GDP, but it still accounts for more than half of the GDP of the 12 former Soviet republics.
- Although neither Transnistria nor the Donbas has a Russian ethnic majority, their cultural, civilizational and linguistic links with Russia are extensive. In South Ossetia and Abkhazia, the linguistic and cultural links to Russia are important because their national languages are so small that exclusive reliance on them would marginalize societies where most members possess Russian passports anyway.

Living with stalemate

Conflicts in another region, Sub-Saharan Africa, provide a clearer picture of the prospects for resolving protracted conflicts in Europe. There is agreement that the chances for resolution improve when warring parties reach a state of mutually hurting stalemate and seek to attenuate the pain of maintaining the status quo by negotiating. This would seem to apply to the conflicts in the former Soviet Union; however, the situation is far more complex for a variety of reasons. Most important, these conflicts cannot be isolated from the roles of external players.

All of these protracted conflicts include external participation/involvement. External actors' roles are multilevel and multilayered. These include guaranteeing one party to the conflict — most often a separatist entity — security, economic contributions and access to internationally recognized travel documents. Hence, external sources offset the pain and cost of stalemate. Russia plays this role in most conflicts in the post-Soviet region. In Abkhazia and South Ossetia — two entities that Russia recognized as independent states, helping them go beyond de facto separation — this role is clearly visible, though Moscow could not generate much international support for its action. In Ukraine, the situation is similar; Crimea was annexed by Russia and now lives on and contributes to the Russian budget. The Donbas would not survive independently and increasingly looks like a Russian economic outpost, while Transnistria has been in a similar situation for decades. Nagorno-Karabakh is the only protracted conflict in which Moscow does seem to be a direct contributor to its perpetuation. There, Moscow has been contributing to crisis stability by backing Armenia to balance Azerbaijan's military superiority, thus guaranteeing Armenia's continued control of the territory it occupied by force.

An ethnic Armenian soldier in the Nagorno-Karabakh defense forces adjusts the aim of an artillery piece during a flare-up in the long-simmering conflict with Azerbaijan. REUTERS

In most cases, Russia is an indispensable external factor in guaranteeing that the parties remain in the status quo. However, Moscow does not see its role as external. It does not view the end of the Soviet Union as the end of its controlling interests in the region and has maintained a patronizing role. Russia moved from ignoring the post-Soviet space in the first half of the 1990s to a policy of dominating relations within "its" region for more than two decades since. Russia's primary objective has been to keep outside powers from interfering in regional conflicts. Aware of its relative weakness and perceiving that change would not be in its interest, Moscow long favored the status quo. However, due to its economic upswing supported by higher prices for its main export commodities, primarily oil and natural gas, Russia felt increasingly entitled to use its power to interfere and change the status quo to its

Masked Russian soldiers take up positions around a Ukrainian military base in Crimea in March 2014, as Russia illegally occupied and later annexed the territory. GETTY IMAGES

liking. This is often described as a move from Russian revisionism to revanchism. It is fully understandable that a great power tries to capitalize when circumstances are favorable; however, using force to realize its political objectives crosses a line when it deprives its partners of political independence. Russia did this in Georgia in 2008 and has been doing so in Ukraine since 2014. A country that is disrespectful of the sovereignty of its neighbors undermines its argument for a sovereignty-based system. This classic double standard is familiar in the international system and in the structural version of the realist school of international relations.

Russia's influence

How should Russia's involvement in the post-Soviet conflicts be assessed? Is Russia simply trying to maximize its power to assert itself as an indispensable regional leader? Or is Russia trying to establish a ring of loyal partners and allies in its natural sphere of influence? Did Russia cause or contribute to protracted conflicts in order to curtail the influence of other external players from the West? All of these factors play a role.

For more than 15 years, Russia has maintained that the international system should be multipolar and Russia should be one of its poles. Although there can be a multipolar international order without Russia forming one of its poles, it is understandable that Moscow regards itself as entitled to that position. In fact, Russia is a de facto power because of its geographical size, nuclear arsenal, diplomacy and hydrocarbon reserves. However, Russia is unimpressive in other areas: It is not a role model for most countries, nor does it produce world-class consumer products, be it automobiles, mobile phones or computers. Although its public diplomacy has improved greatly, the annexation of Crimea and Russia's subversive military presence in the Donbas undermine its credibility. Nevertheless, Russia knows that relative power matters and seeks to maximize it.

Russia needs followers in order to increase its weight in the international system. Although it has massive influence in some countries, e.g., Syria or Iran, the number of staunch followers remains limited. It is easiest to gain influence in its natural sphere, the post-Soviet space. However, Russia alienates some partners with an impatient, often reckless coercive policy. Some countries are reluctant to associate with Russia beyond what is absolutely necessary. Others, short of alternatives, such as Belarus, Tajikistan and the Kyrgyz Republic, follow with more or less hesitation, while still others are affected by protracted conflicts, such as Armenia and Moldova. Consequently, a number of other factors contribute to enticing states to follow Moscow, such as small economies, poor natural resource bases

and insufficient support from other sources of political and economic power. The economies of Armenia, the Kyrgyz Republic, Moldova and Tajikistan are smaller than $30 billion each, making their dependence on Russia existential. The largest five economies in the post-Soviet space are all natural resource exporters and, with one exception, producers. This means that no post-Soviet state has found its way to self-enrichment, though Georgia (No. 6 among the 12 post-Soviet states) has made progress. Therefore, protracted conflict alone does not result in voluntary self-subjugation. Rather, protracted conflicts play a contributing role to the acceptance of Russian superiority, though each case is different and requires independent analysis:

- Armenia's case is crystal clear: Without the backing of Russia, both bilaterally and as a member of the Collective Security Treaty Organization, it would be enormously difficult for Armenia to withstand Azerbaijan's military and economic advantages and maintain control of Nagorno-Karabakh.
- For Moldova, it would be difficult to compensate for the massive asymmetry between the parties and its multidimensional dependence on Russia; however, with skillful politics (attracting the European Union as an alternative trade partner) and multilateralization of dispute settlement related to the Transnistria conflict, Moldova has been able to avoid full dependency.
- Georgia has lost its secessionist territories, Abkhazia and South Ossetia, and there is practically no chance that they will return to Georgian rule. However, Georgia has been developing rapidly since reforms initiated by former President Mikheil Saakashvili. In spite of a somewhat controversial record, Georgia will remain the state that has successfully broken out of the post-Soviet paradigm. It has massively reduced corruption, consolidated good governance and attracted foreign direct investment on a level unique for a country without large reserves of natural and energy resources.
- Ukraine's protracted conflicts have been relatively short-lived and thus it may be premature for predictions. However, in spite of certain governance shortcomings in Kyiv, Ukrainian society has demonstrated a cohesion that curtails the chances of returning to the political *status quo ante*. Nevertheless, it could be concluded that the territorial status quo has changed, because Crimea may well remain part of the Russian Federation, despite the illegality of the annexation. It is important to note that the conflicts between Ukraine and Russia have not resulted in increased influence of Moscow over Kyiv, although they are elevating Russia's international notoriety.

A country that is disrespectful of the sovereignty of its neighbors undermines its argument for a sovereignty-based system.

In sum, protracted conflicts clearly result in increased Russian influence as an intervening partner or direct party. This offers other external players some room to maneuver, although it would be best not to imply that a geopolitical contest is under way in the post-Soviet space between Russia and the West.

The conflict management mechanisms dedicated to protracted conflicts are unsatisfactory. These conflicts are being managed, rather than resolved. This is understandable when the Organization for Security and Co-operation in Europe (OSCE) plays a major role. The OSCE is an inclusive institution where every participating state has an equal role in decision-making. Its decisions are made by consensus and every state has a veto. The organization does not have strong enforcement mechanisms. Hence, decisions fall to the states and their willingness to seek resolution. Furthermore, in many cases the status quo is not sufficiently unbearable to precipitate change. This certainly applies to Abkhazia, South Ossetia and Crimea, three conflict zones where the new territorial status quo holds, and it is largely true for Transnistria. In the remaining two cases, the situation is volatile and the conflicts are furthest from being frozen; however, the status quo has held in Nagorno-Karabakh for 23 years and, irrespective of the heated propaganda exchanges between Baku and Yerevan, there is some accommodation. In the Donbas, finding a resolution is more complicated because the direct and indirect parties want to change the political, but not necessarily the territorial, status quo.

Conclusions

- Most protracted conflicts have not reached the phase of "mutually hurting stalemate," inhibiting sufficient motivation to find a resolution. If external players — who may not always regard themselves as external to the conflict — stop exerting influence and support, this could change. However, it may result in "defreezing" the conflict and a return to violent escalation.
- Political actors may keep the conflict on the domestic political agenda and develop support for their agenda by declaring an external adversary. Nevertheless, people act in their best interests. The longer a protracted conflict holds, the more societies adjust and people find ways to get on with their lives.
- The involvement of Russia — the only great power that does not regard itself an external actor — in protracted conflicts has seldom resulted in additional leverage over the conflicting parties.
- Conflict management mechanisms and institutions stop short of effectively seeking resolutions. The power of international organizations is often too limited to achieve radical change, and that contributes to the perpetuation of the conflicts. □

Hybrid War AND HYBRID THREATS

Coping with conventional and unconventional security challenges

By ***Dr. Sven Bernhard Gareis***
German deputy dean at the Marshall Center and professor of international politics at the Westfälische Wilhelms-Universität

It is not a new phenomenon that states at war employ a broad array of instruments besides military forces to achieve their objectives. Deception, propaganda, information campaigns, and irregular or covert operations have always accompanied conventional warfare. These measures aim to demoralize soldiers fighting on the front line and decrease domestic support for the war. They target the human psyche by raising anxieties and fears, seeding doubts, questioning the legitimacy of governments and institutions, and splitting national cohesion along social, cultural, religious or ethnic lines.

In this regard, the hybrid war that the Russian Federation has been waging in Ukraine since 2014, and the threats that it poses to other countries in its nearer or more distant neighborhoods, do not constitute a genuinely new concept of warfare. On the contrary, the doctrine that Russian Chief of General Staff Vladimir Gerasimov presented in 2013, and that has been systematically used in Ukraine since, is based on the assessment that Western countries — first and foremost the United States — have used financial support to opposition parties, deceptive information campaigns and "color revolutions," in conjunction with economic incentives and military posture, to change the security environment in the post-Soviet space to their favor and to Russia's detriment. Based on this perception, Russia is justifiably responding to Western challenges.

Targeted states such as Ukraine — and the West at large — are less surprised by the so-called Gerasimov Doctrine's line of attack than by the degree of precision and determination with which the Russian government under President Vladimir Putin deploys its military and nonmilitary capacities in domains such as cyber, information technology, public opinion, diplomacy and covert military operations. Russia's relative success in Ukraine is largely due to the latter's weak national cohesion, political culture and institutions,

Macedonians protest in front of the EU building in Skopje in May 2017, a few days after violence erupted when angry nationalist protesters stormed parliament. Societal fissures make countries more vulnerable to hybrid tactics. AFP/GETTY IMAGES

and to the West's inability to appropriately respond to Russian aggression.

This helplessness has its reasons: Hybrid measures are purposely applied beneath the threshold of conventional warfare. Unlike soldiers, armored divisions or fighter aircraft crossing borders, it can be difficult to attribute responsibility for cyber attacks or other nonmilitary assaults. There are blurred borders and gray zones: Is Russia supporting separatist movements in eastern Ukraine or has it launched a military aggression against a sovereign country? The European Union, the U.S. and other countries imposed bearable sanctions on Russia, but avoid more energetic action since many Western countries maintain strong economic and political ties with Moscow. It seems as if the West has tacitly accepted that Crimea will not return to Ukraine in the foreseeable future, and eastern Ukraine is still war-torn while the Minsk Agreement has not successfully been implemented.

Among the most effective elements in the hybrid war toolbox are information campaigns that aim to manipulate public opinion, damaging the adversary system's reputation and conveying the aggressor's own narratives.

Against this backdrop, how can states, societies and alliances defend against warfare that does not strive for territorial gains or military dominance, but rather to destabilize, if not destroy, the societal order of a nation or region? The complexity of hybrid warfare requires complex responses and a different set of instruments. However, what is needed first is a thorough analysis of the hybrid threats and a sober assessment of the vulnerabilities within states and societies.

Hybrid warfare and hybrid threats

Since 2014, the terms "hybrid war" and "hybrid threats" have increasingly been used in international security policy discourse. However, with limited exceptions, there is no common definition or concept in political practice or academia that can be used to reliably designate a situation as hybrid war — and therefore no set of political, military or legal measures and procedures that states or organizations can invoke in response to the threat.

Hybrid warfare can be described as a combination of military force — open and covert — and any nonmilitary means that could harm a state, society or international organization such as the EU or NATO. While such means often complement classic military operations in conventional wars, they are essential instruments in hybrid warfare and often outweigh military efforts. According to Gerasimov, the ratio of military to nonmilitary means should be 1 to 4. As elements of an integrated strategy, the means are systematically and flexibly applied where they fit best. In the case of military action, this can be special forces operations by "little green men" without identifying insignia, or covert support of insurgents. Such operations allow the attacker to deny direct involvement and to make the situation as unclear as possible.

Cyberspace is an ideal realm for hybrid warfare. It transcends classic borders, it interconnects private, public, economic and administrative areas, and it is — despite enormous efforts by powerful states such as the U.S. and China — difficult to control. Cyberspace offers convenient commodities, such as globally interconnected infrastructure, allowing for real-time communication for public, private or individual actors that has boosted international exchange, trade and commerce. At the same time, the far-reaching dependency on these technologies in all areas reveals increasingly existential vulnerabilities. The virtual nature of cyberspace allows all kinds of actors to launch serious attacks that cause considerable damage to individuals, organizations and states and that carry a low risk of being traced. As an instrument of hybrid warfare, cyber attacks can confuse or disrupt communication infrastructure, cause temporary paralysis of public life, and contribute to an overall climate of uncertainty and fear. It can undermine the legitimacy of governments that are unable to protect societies from very real cyber threats. Defending public and economic infrastructure against attacks has become an everyday challenge.

Cyber espionage and cyber crimes pose growing threats to nations, businesses and individuals. The disclosure of hacked information from the electronic communications of prominent politicians can influence elections, as can attacks on electronic voting systems. As revealed by the 2016 U.S. presidential elections, democratic countries must become more attentive to the perils of interference from cyberspace. Revelations, such as those from WikiLeaks, can have negative impacts on national security. Destructive malware such as Stuxnet — allegedly launched by the U.S. to destroy central parts of the Iranian nuclear program — have proven to be a lethal weapon in military arsenals, again without the possibility of clear attribution.

Among the most effective elements in the hybrid war toolbox are information campaigns that aim to manipulate public opinion, damaging the adversary system's reputation and conveying the aggressor's own narratives. In the globalized and digitalized world, such campaigns are not confined to a single target. In Ukraine, Russia countered the 2013-2014 Maidan protests against then-President Victor Yanukovych with a massive campaign that denounced the demonstrators and new leadership (after Yanukovych fled the country) as fascists and sought to compromise their legitimacy and reduce public support in Western countries. Of course, Ukraine is only one theater in the broader Russian hybrid campaign against Western influence in the region. The tactics used there were also meant to weaken Western cohesion in assessments and responses to hybrid threats.

Children study at a school in Marinka, near the front lines of Ukraine's smoldering war in November 2016. Functioning and trustworthy institutions are necessary for a stable society.
AFP/GETTY IMAGES

Information campaigns show manifold faces and use versatile channels. There is blunt propaganda, and there are professionally designed media, such as Russia Today, that present fake news in the guise of serious information. There are troll commentators on online media, reputed experts' comments in popular mass media, and well-funded think tanks and foundations, such as the Dialogue of Civilizations Research Institute in Berlin, that help set agendas for public discussions. An old Cold War-proofed instrument is the creation of message multipliers by financially supporting local movements or parties that are dissatisfied with the political or socio-economic order in their countries.

The primary purpose of information campaigns is to undermine public trust in institutions, structures and procedures in the targeted states and societies, be it by "fake news" or by creating confusion. After the downing of Malaysian Airlines Flight 17 over eastern Ukraine, Moscow attempted to overwhelm the global public's capacity for fact-based assessment and judgment by pushing a plethora of explanations and interpretations — many of them fully or partially contradicting each other. Blurring borders between facts and fiction erodes the basis for serious debate.

How do hybrid threats function?

As already stated, the most important objective of hybrid warfare is to create confusion and destroy trust. Hybrid measures target the foundations of the human psyche: to feel safe and secure is a fundamental desire of every individual. This desire goes far beyond the guarantee of physical survival — human beings have the need to feel respected and to enjoy equality and justice, not only in legal terms, but also with regard to social, economic, cultural, ethnic and religious aspects.

At the national level, these aspects form the foundation of the concept of societal security, which guarantees fair and discrimination-free treatment for all. In their landmark book, *Why Nations Fail: The Origins of Power, Prosperity, and Poverty*, Daron Acemoğlu and James A. Robinson describe those societies as inclusive, in contrast to extractive forms of societal order, which prioritize the well-being of certain social groups (often referred to as elites) at the expense of others.

The "World Happiness Report 2017" gives empirical evidence to this finding. It highlights the juncture between personal and social happiness and its global ranking shows the close correlation between happiness, and peace and stability. Consensus-oriented Scandinavian nations are the happiest, while war-torn nations in Africa show the lowest degree of happiness. Acknowledging that a correlation does not necessarily indicate a causal relationship between variables, the positive impact of inclusiveness on societal security appears at least to be plausible.

In this respect, the more inclusive and just a society is perceived to be by its members, the more stable it is. And vice versa: deeper social splits and political polarization indicate less trust in institutions, and the more corrupt a system is perceived to be, the more fragile is the society, making it more prone to hybrid intervention from outside.

When social inequality is not accepted as a just outcome of fair competition under equal conditions for all members of a society, feelings of injustice and grievances over discrimination can be easily exploited to widen gaps along social, ethnic or religious lines. As a result, states and societies may disintegrate into antagonistic camps that are no longer able to communicate with each other. The perception of disenfranchisement often makes those groups easy prey for so-called strong leaders with clear-cut and simple "solutions" to increasingly difficult problems. This is compounded by a global trend in the use of media and information: To escape the complexity of problems, more and more people withdraw into filter bubbles that admit only information that reinforces existing preferences, attitudes, opinions or behavior. To avoid cognitive dissonance, contradictory facts or divergent

Latvian soldiers participate in Operation Hazel exercises at the Adazi training field. Military readiness is an important but relatively small facet of resisting hybrid attacks. REUTERS

interpretations are actively excluded from consideration. Consider how an analysis of internet users' search behavior is utilized to create algorithms that propose only goods, services or information that fit existing patterns. With political communication, agitators can reinforce dissatisfaction and foment radicalization in thoughts and action.

Russia capitalized on Ukraine's fragile national identity and seized the opportunity of political transition to carry out a professionally orchestrated hybrid campaign, successfully stirring up resentment within the Russian-speaking populations in Crimea and eastern Ukraine. It is not difficult to predict which leverage points Russia may try to use in other countries outside and within NATO or the EU. In the U.S. and France, Russia pushed "anti-establishment" themes in the respective presidential campaigns of 2016 and 2017. In many European countries, nationalist and xenophobic parties and movements have had considerable success in contesting the benefits of European integration, thus reinforcing the EU's internal crises. Polarization, distrust, anger, and even hatred, weaken states and societies, open avenues for hybrid interference from outside, and thus constitute serious threats to national integrity and stability within individual countries, and to regional and international orders.

Countering hybrid threats

Hybrid measures often overwhelm the defense capacities of a single state and/or challenge groups of states or regions. They require concerted responses both in identifying threats and effectively countering them. Since hybrid threats are primarily of a non-military nature and use versatile guises and channels to make an impact, any alliance or security organization must use analytical capacities to assess whether suspicious incidents are isolated phenomena or are indeed elements of a hybrid strategy. To this end, it is indispensable to further interagency exchange of data, findings and assessments to facilitate analysis of a multitude of distinct events and cases. It is primarily a national task of member states to arrange interagency cooperation among military, police, intelligence services, emergency management authorities and civil administrations. Institutions like the EU Hybrid Fusion Cell, within the EU Intelligence and Situation Centre, or the newly established Finnish Centre of Excellence for Countering Hybrid Threats (supported by several EU and NATO members), are bodies that collect and examine reports and assessments from member states and common agencies that can be used to develop collective countermeasures.

At its Wales (2014) and Warsaw (2016) summits, NATO re-established a focus on collective defense and deterrence. Under the Readiness Action Plan, the Alliance established the Very High Readiness Joint Task Force and deployed

small military contingents to Poland and the Baltic states as an enhanced forward presence, designed to show force to a potential aggressor, as well as to demonstrate the solidarity and determination of its member states. Partner nations such as Ukraine and Georgia receive support in fields such as strategy, doctrine and education, military training assistance, and the (limited) provision of military equipment and nonlethal weapons. Military measures are necessary and crucial to counter the military dimension of hybrid aggression. However, according to Gerasimov's 1 to 4 ratio, the military is only one instrument in the defense toolbox — and most probably not the one of primary importance.

In addition to the EU Joint Framework on Countering Hybrid Threats, the EU's decisive strength lies in the social and economic foundations for societal security that it offers to member states. The relatively high degree of freedom, economic opportunity, welfare, functioning institutions, rule of law and nondiscrimination make EU member states with large ethnic minorities less prone to hybrid exploitation of societal splits and cleavages. There is not much an aggressor can offer to outweigh the tangible advantages of considerable welfare, a stable currency or an EU passport with the freedom of movement it guarantees.

As the successes of nationalistic movements in many countries illustrate, EU membership does not provide immunity against external actors stirring up and exploiting dissatisfaction. The likelihood of grievances escalating to unrest or even revolution, however, is very limited. To the contrary, the EU provides a political and legal framework that helps tame political actors and mitigate problematic developments in countries such as Hungary or Poland, where democratic achievements are currently at stake, and bring them back to common standards of democracy, societal security and stability.

Building resilience

As in the case of hybrid warfare, there is no clear definition of resilience. In general terms, resilience describes the ability of a system or an organism to maintain its basic, vital functions, even after having suffered severe damage. In terms of national security, resilience means a country can absorb a military strike, a terrorist act, a cyber attack or a series of lower-scale actions across the spectrum of hybrid warfare and continue, as much as possible, to function normally.

In democratic states, this requires maintaining the balance between necessary security measures and individual freedoms and civic rights, while not transforming into a surveillance state. In this regard, the public's trust in good governance and stable institutions is extremely important. To this end, states must create capable security agencies that can identify and tackle threats and mitigate the consequences of hybrid attacks. To be credible, these institutions need to be strong in analysis and assessment, effective in taking countermeasures, and interconnected with national and international partners.

Effective security agencies are indispensable to defend against hybrid threats. It is, however, equally important to any national security strategy to start with the insight that hybrid actions capitalize and reinforce dissatisfaction, grievances and complaints within states and societies, but they do not produce or import them. Hence, building resilience begins with a relentless analysis of a state's own weaknesses and vulnerabilities. Government, elites, political parties and social groups must find sober answers to the questions inherent in guaranteeing societal security.

The most important indicator of inclusivity is the degree of trustworthiness that political and societal institutions and structures enjoy among the citizenry. This depends on democratic legitimacy and on procedures that are based on the rule of law and that guarantee integrity and transparency. This includes effective efforts to detect and fight corruption, nepotism and any other arbitrary access to resources of power and wealth.

In this context, governments and civil society must provide equal opportunities for all citizens to participate in public, social and cultural life. Are there complaints of discrimination and how seriously are they taken? If there are cleavages and disruptions, what can be done to effectively enhance societal integration? Building societal resilience depends on how serious and trustworthy a government's integration efforts are perceived by the individuals and groups concerned. The most important characteristic that distinguishes a mature and successful democracy from a potentially unstable political system is how the majority treats minorities and how the powerful treat the weak.

How a society deals with the challenges of disinformation, fake news and propaganda can be considered a valid litmus test of its resilience. Responses to information campaigns cannot be confined to counterpropaganda or "strategic communication." As an essential element of hybrid warfare, false information is particularly successful if political communications and public opinion are segregated into partisan camps that live in their own filter bubbles. It takes effort and time to bring people together to discuss solutions to common problems. The fundamental prerequisite is, again, trust and credibility. The less inclusive a society is the more susceptible it is to manipulation of dissatisfied individuals and groups. If state institutions and civil society live up to the values of free and inclusive societies — based on integrity, transparency, rule of law, trustworthy institutions and free media — they can blunt hybrid warfare's sharpest sword.

Conclusion

Hybrid threats are not a new phenomenon, but in this globalized world, with its breathtaking development of ever faster communications, its impacts become massive and dangerous. They pose new challenges for national security policies and agencies — but at the same time, adequate defensive measures open immense opportunities for societies. True resilience requires a certain degree of satisfaction and happiness among all citizens. Responsible governments and civil society actors must take into account the close nexus of societal and national security and strive to make their citizens happier and their nations stronger. □

From Calamity to COORDINATION

How a botched 1970 defection request led to a 'whole-of-government' approach to crises

By Brian Wilson, deputy director of the Global Maritime Operational Threat Response Coordination Center, and Wayne Raabe, U.S. Department of Justice, Criminal Division

In December 2016, the George C. Marshall European Center for Security Studies invited government officials from more than 50 countries to examine issues related to countering transnational organized crime. Because security challenges frequently include multiple ministries, the development of frameworks that formally align response efforts represented a core focus of this innovative, two-week course in Garmisch, Germany.

A seminal event in this "whole-of-government" coordination process occurred in 1970 when Simas Kudirka, a Lithuanian sailor, sought to defect to the United States by leaping from his Soviet-flagged vessel onto a U.S. Coast Guard cutter off the coast of Martha's Vineyard. Resolving this situation would normally require collaboration by several ministries operating under separate chains of command. At the time, however, no documented framework existed within the U.S. to compel information sharing or synchronize decisions. A series of missteps culminated in Soviet "sailors" removing the merchant seaman from the cutter in U.S. territorial waters, with the crew of the cutter powerless to intervene.

Cmdr. William Goetz, right, welcomes Simas Kudirka aboard the U.S. Coast Guard Cutter Vigilant in November 1974, four years after Soviet sailors dragged Kudirka from the same ship to thwart his attempted defection to the United States.

THE ASSOCIATED PRESS

The mishandled Kudirka event sparked transformative changes within the U.S. government to ensure timely information sharing and coordinated responses to nonmilitary events and threats. The event also resonated with Lithuanians, who viewed Kudirka as a freedom fighter. The participation of officials from Lithuania and the U.S. at the December 2016 Marshall Center program, Countering Transnational Organized Crime (CTOC), provided a unique opportunity to assess the enduring impact of Kudirka, whom the Soviets tried for treason and sentenced to 10 years in a labor camp. Senior-level diplomatic talks culminated in a Soviet decision to release Kudirka from prison after four years and he emigrated to the U.S.

Lithuanian Zydrunas Velicka, who attended the course, first heard of Kudirka when he was at secondary school in 1994, four years after Lithuania proclaimed its independence from the Soviet Union. "It was a lesson about Lithuania's resistance against the Soviet regime," Velicka recalled. "Kudirka is regarded as a participant in our resistance against the Soviet occupation."

In 1970, back in the U.S., senior Coast Guard officers were widely blamed for the botched Kudirka response. U.S. Rep. Samuel S. Stratton asserted, "It is obvious that the person primarily responsible for this shocking, stupid and probably very costly fiasco was the rear admiral in charge of the Boston district of the Coast Guard, who gave the order. … The longer we delay taking appropriate disciplinary action in this case, the worse we look in the eyes of freedom-seeking people everywhere."

Eight congressional hearings, as well as executive branch inquiries, highlighted misguided individual decisions. But the primary causes of the Kudirka outcome were a lack of national-level coordination guidance, poor training and the absence of an articulated policy. These findings led to a presidential directive on alignment for intergovernmental response to nonmilitary incidents. In 2005, as part of the National Strategy for Maritime Security, the whole-of-government process expanded to include security threats as well, such as piracy, terrorism and the transport of weapons of mass destruction (WMD).

The U.S. government's maritime event coordination process, the Maritime Operational Threat Response (MOTR) Plan, is based on the painful lessons of Kudirka's asylum request. Mechanisms that compel information sharing and align responses present tremendous governance challenges, in part because ministries are not necessarily structured — or even authorized — to communicate and coordinate with one another.

The MOTR Plan is one of about 15 that has emerged globally since 2005 to support national-level maritime response alignment. Though these frameworks are substantively different, they share a similarity: Most don't supplant or replace agency authorities, but instead support synchronized responses among ministries. Characterized as horizontal coordinating mechanisms, these processes generally function under a "unity of effort" construct rather than "command and control." MOTR, for instance, established a process to integrate multiple ministries to share information, develop courses of action, align responses, and identify lead and supporting agencies through a network of national level command/operations centers, instead of a "bricks and mortar" joint command center. A 2006 FBI Office of the Inspector General report concluded, "We believe that the MOTR's efforts … help meet an existing policy void."

If there is not a formal process, personnel in one agency may not know whom to contact in other agencies and may not be empowered to make a decision or even participate in a response. Information discarded by one agency may be the critical piece for another to identify a threat. Even with information flowing effectively, there may be uncertainty about whom to involve, what is unfolding and what are the next steps.

A documented framework defines agency roles and ensures information sharing across ministry lines. Further, ensuring that a government speaks with one voice represents an overarching goal. Without a structured process, the potential for uncertainty greatly increases as to which departments and agencies should be included in response planning and execution, as well as which agency should lead and which should provide support.

Discussions in a structured process, for example, could include whether to board a ship, law enforcement action for the crew/passengers, and disposition of the cargo and/or the vessel following an interdiction. Agency authorities, capabilities and responsibilities, and courses of action are addressed, culminating in a decision regarding the desired outcome. Coordination activities should seek to generate the most important outcomes — an agreed-upon summary of the facts and desired national outcome(s) — and identify uncertainties and ambiguities, assigning their resolution to participants. The response to a threat could be resolved in one coordination activity or could span several events. If utilized, the facilitator is responsible for tracking follow-through action items.

The safety/security response spectrum increasingly involves a number of government ministries, including the military, law enforcement and the diplomatic corps. More agencies are involved because threats are more complex, authorities can be more widely distributed throughout a government and the end-state is often the courtroom. Responses to a situation in which a dosimeter check on cargo registers positive or an inbound aircraft carries a passenger who may have an infectious disease, for instance, could involve multiple ministries. Moreover, combating piracy, terrorist activity, drug trafficking, WMD and migrant smuggling all have the potential to involve government agencies that operate under different chains of command, with separate authorities, separate responsibilities and separate funding.

As national-level interagency maritime threat/event response frameworks become an integral part of the security landscape, unambiguous head-of-state direction, agency support, frequent use and civility must be the norm. Other enablers include leveraging multiple agency authorities, capabilities and competencies to form a networked response; the ability to address emerging (and at times, unexpected) threats; 24/7/365 capability; documenting and distributing decisions; training and professional development for those involved in the process; engaging diplomatic officials early; and promulgating operational, implementing guidance. The focus on whole of government is emblematic of a changed security, and response, environment. The December 2016 CTOC program notably supported discussions on both the challenges and goals in developing a structured framework that achieves unity in supporting the timely identification of a threat and the aligned response.

Frequent use of the whole-of-government mechanism and workshops that bring together nontraditional participants and feature scenario-based training improve coordination implementation and build trust among participants unaccustomed to working together and lead to improved coordination when faced with actual operations. Workshops can help to:

- Identify agencies within your government that could be involved in a response to transnational criminal activity, from the beginning to the end of a particular event.
- Draft a definition of "whole of government."
- Describe how "unity of effort" varies from "command and control."
- Identify impediments that prevent information sharing outside a ministry (yet within government).
- Identify scenarios based on prior experiences.

To achieve a timely, aligned and effective response framework, it is essential to continually examine productive responses and those that are mishandled. The mishandled cases, due to faulty communications, procedural mistakes or human error, will inevitably receive considerably greater scrutiny.

Velicka added that while he knew Kudirka's return to the Soviets generated a negative response within the U.S., the CTOC presentation on its enduring impact was informative. "At the eighth decade of the 20th century, Simas Kudirka became for many Lithuanians a symbol of freedom, expressing the hope of all peoples to free themselves from Soviet oppression," he said. "That this event somehow affected further U.S. interagency cooperation and that later this accident was taken into consideration was new for me."

Almost half a century after the confused response to Kudirka's defection attempt, governance lessons with resonance today include: the imperative of national-level guidance to align multiple agencies involved in the response spectrum; strong ministry involvement and support; frequent training and familiarization; and clearly understood implementing guidance. The challenge — and goal— is developing a structured framework to achieve unity of effort to support the timely identification of a threat and aligned response. □

ISIS in Turkey

THE GOVERNMENT'S RESPONSE HAS GLOBAL CONSEQUENCES

By Ahmet S. Yayla, Ph.D., George Mason University

The Reina nightclub attack, which occurred in the early hours of New Year's Day 2017 in Istanbul, Turkey, and the counterterrorism operations after the attack provide valuable security lessons. The attacker, Abdulkadir Masharipov, spent a year in a sleeper cell in Konya, Turkey, before receiving orders from his emir in Raqqa, Syria, using the Telegram app. He not only carried out an attack in the name of ISIS, killing 39 people and wounding many others, but also dodged police scrutiny at the scene by pretending to be one of the victims. ISIS has a heavy presence in Turkey, with several established cells and safe havens, and it has been openly threatening Turkey since the al-Bab military campaign in Syria. Turkey is a bridge between the East and West, and the danger of Turkey becoming the gateway for European terrorist activity cannot be ignored. With ISIS starting to lose vast territories in Syria and Iraq, Turkey's capacity to counter terrorist threats and stem terrorist activity within its borders is critical for global security.

TERROR AND TOLERANCE

Turkey has been afflicted by terrorism for a long time, costing over 40,000 lives in the past 40 years. When the Syrian uprising against President Bashar Assad began in 2011, Turkey was enjoying a statistically peaceful era, with the lowest number of causalities from terrorism in its recent history. However, this historically less-violent period quickly deteriorated due to new regional conflicts and Turkey's flawed domestic and international policies. Turkish leaders considered the Syrian uprising to be an opportunity to further their interests in the region, and it effectively promoted a prompt regime change by supporting radical Salafist jihadist groups in Syria. In the beginning, this policy might have seemed appropriate because most Turkish support went to the Free Syrian Army, which was considered the foundation of the regional and local resistance. But radical Salafist jihadist groups, including the al-Qaida-affiliated Jabhat-al Nusrah (now called Jabhat Fateh al-Sham, or JFS), Ahrar al-Sham, the Nour al-Din al-Zenki Movement and, ultimately, the Islamic State (ISIS), eventually received Turkish-facilitated assistance.

A Turkish police officer stands guard a day after the Reina nightclub attack.

AFP/GETTY IMAGES

A bomb exploded near the homes of judges and prosecutors in a mainly Kurdish town in Sanliurfa province in southeastern Turkey in February 2017. THE ASSOCIATED PRESS

Iranian-Turkish businessman Reza Zarrab is detained in 2013 by Istanbul police investigating corruption, a chronic problem in Turkey. Three years later, U.S. officials charged him with conspiring to evade sanctions against Iran, money laundering and bank fraud. AFP/GETTY IMAGES

ISIS has been advancing its presence in Syria ever since. It declared a caliphate at the end of June 2014 and immediately started capturing major routes from Turkey to Syria, becoming Turkey's new neighbor to the south and controlling some border gates and smuggling routes. As ISIS was becoming a major enemy of the Kurdistan Workers' Party (PKK) and Assad, Turkey adopted a policy of nonintervention, allowing foreign fighters passing through to join ISIS and other radical groups in Syria. This policy has resulted in the passage of over 25,000 foreign fighters through Turkey and has allowed several radical groups to carry out their logistics and operations within Turkey's borders.

Turkish support of ISIS has played a critical role in its operations. Had Turkey not been so tolerant of ISIS' activities within its borders, including the recruitment of thousands of foreign fighters, ISIS would not be as powerful as it is today. Enabled by Turkish policy, ISIS empowered itself beyond imagination in a very short period. Turkey and ISIS did not consider each other enemies, at least not openly, until the Turkish military and the Free Syrian Army conducted the al-Bab offensive. Al-Bab was the turning point from which ISIS began openly targeting Turkey for attack in its magazines and through the statements of its leaders. The Turkish government did not label ISIS a terrorist organization until the beginning of 2016. Even after attacks in Turkey, then-Prime Minister Ahmet Davutoglu openly failed to call them terrorists, stating, "They are a bunch of frustrated young kids." The relationship between Turkey and ISIS started to sour at the beginning of 2016, as Turkey reluctantly curtailed its support under pressure from the Obama administration.

Turkey began showing signs of domestic political and economic turmoil starting in 2014, mainly due to the Istanbul Police Department's investigation of corruption and bribery allegations against the ruling party's inner circles. President Recep Tayyip Erdogan, claiming the investigation was a coup against his rule, immediately started purging and firing police officers, chiefs, prosecutors and judges involved in the investigation. However, in New York, the United States Justice Department and the Federal Bureau of Investigation carried out a parallel investigation. It led to the March 2016 arrest of Reza Zarrab, one of the main suspects and detainees in the Istanbul investigation, on charges of conspiring to evade U.S. sanctions against Iran, money laundering and bank fraud. The U.S. investigation and Zarrab's arrest lent validity to the Istanbul investigation.

Throughout 2014 and 2015, the purges and arrests reached police departments across Turkey, replacing experienced counterterrorism, intelligence and organized crime divisions with new officers and chiefs loyal to Erdogan. Consequently, ongoing counterterrorism operations against ISIS, al-Qaida and other jihadist terrorist organizations were halted as newly appointed police officials focused on quashing any pending investigations of the politicians or people close to them. In fact, several police officers and prosecutors were arrested for investigating the flow of weapons and support operations provided to terrorist organizations, including the infamous Adana Highway scandal involving Turkish National Intelligence trucks carrying weapons to Syria and the Van Police Department's operation of the local Humanitarian Relief Foundation, which supported terrorists through humanitarian relief activities. Because of these government crackdowns on police, there was not a single planned counterterrorism operation in Turkey during 2014 and 2015. The few operations carried out in 2016 were mostly in reaction to specific incidents, with detainees released shortly after capture.

Victims are remembered outside the Reina nightclub in Turkey, where a terrorist killed 39 people early New Year's Day in 2017. The attacker spent a year in Turkey before the assault. THE ASSOCIATED PRESS

However, the crippling of Turkey's counterterrorism apparatus did not end there. When the July 15, 2016, coup attempt took place, Turkey immediately arrested thousands of experienced counterterrorism and intelligence officers, including its police, military, judges and prosecutors overseeing counterterrorism operations. This experience drain further crippled the counterterrorism and intelligence capacity, and terrorist attacks and associated casualties post-2014 have skyrocketed to more than quadruple the rate of the preceding few years.

ISIS took advantage of the political upheaval in Turkey after 2014, increasing its operations and establishing terrorist cells composed of Turkish and foreign ISIS members in Istanbul, Ankara, Konya, Kayseri, Adana, Izmir, Gaziantep, Adiyaman, Sanliurfa, Sakarya and many other locations. Through these cells, ISIS recruited thousands of new members and sent at least 3,000 local fighters to Syria. In addition to recruitment activities, ISIS also established a wide network in Turkey to support its operations in Syria and Iraq. Through this network, ISIS was able to purchase vital materials and transport them to its territories. It contracted factories to produce materials, including missile heads for handmade weapons, explosives, chemicals, electronics for improvised explosive devices, four-wheel drive trucks, 60,000 uniforms, food, electronics and clothes. Ample evidence of these activities is included in recent European Union-funded Conflict Armament Research reports, with details of how Turkey and Turkish companies supported the production of ISIS weapons and explosives. In addition, ISIS was able to sell the oil it was producing in Syria and Iraq to Turkey. In fact, the 2016 release of personal emails of Turkish Oil Minister Berat Albayrak — who is also Erdogan's son-in-law — prove that previous allegations about transferring and selling ISIS oil were true.

In addition to ISIS gaining strength in Turkey and along its borders, 3 million refugees have established themselves throughout the country. Due to Turkey's open border policies for Syrian refugees, anyone fleeing Syria has been welcomed, given Syrian refugee identification and allowed to reside anywhere in Turkey. This migration has been a golden opportunity for ISIS, which has sent hundreds of Syrian ISIS members to Turkey to support ongoing logistical operations, collect intelligence about Turkey and ISIS' enemies hiding in Turkey, transfer funds and carry out assassinations against ISIS enemies. An example is the double assassination in Sanliurfa of activists from Raqqa Is Being Slaughtered Silently, a group that works to expose atrocities committed by Assad and ISIS. Furthermore, terrorists have been sent to Turkey to receive free medical treatment.

THE CELLS

While Turkish terrorist cells are essential to ISIS, the terror group has also established cells with foreign fighters in Turkey. The foreign cells consist mostly of terrorists from the Caucasus region, including Chechnya, Ingushetia and Dagestan, and from post-Soviet Central Asian countries, and also include Russian Turkic people and Uyghur Turks. These cells are led by the Caucasus Emirate of ISIS, Wilayah al-Qawqaz. The Qawqaz terrorists are battle-hardened, experienced and well trained before arriving in Turkey, having spent time on other fronts and sometimes with different jihadi terrorist organizations like al-Qaida in Afghanistan. Qawqaz fighters are the "special forces" of ISIS. In fact, several ISIS defectors have said Qawqaz fighters, especially the Chechens, Kazaks and Uzbeks, are known for their discipline and brutality during attacks, and because of that they usually lead the battles with local Syrian fighters in support. While ISIS has used Turkish cell members mostly for suicide attacks, confrontational attacks have been delegated to the Qawqaz fighters. Caucasus Emirate cells conducted two major attacks in Turkey, including the assault on June 28, 2016, at Istanbul Atatürk Airport and the Reina nightclub attack. These two attacks killed 84 people and wounded over 300. The third formation of ISIS cells in Turkey consists of other foreign fighters, usually from Europe or, in some cases, North Africa. However, these cells mainly act as safe havens and are used to facilitate the transfer of foreign fighters.

The leadership and hierarchy of ISIS cells and establishments in Turkey vary. City-level emirs (commanders) lead the Turkish cell structure and the support base; there are also regional emirs and an emir in charge of all of Turkey. While the city and regional emirs reside in Turkey, the emir in charge of Turkey does not. In addition to this vertical hierarchy, there are individuals in charge of recruitment activities: *dawah* leaders (teachers of ideology and indoctrination), financial emirs, those who facilitate the passage of foreign fighters, border emirs, logistical support directors and facilitators, and *zakat* (almsgiving) collectors. While these leaders are tied to the Turkish emirate, the Qawqaz fighters and foreign cells are independent of the Turkey-based ISIS cells and do not communicate with them. Qawqaz fighters are chosen and assigned by the Caucasus Emirate of ISIS, and the respective

emirs in Raqqa manage the foreign cells. This is a security measure so as not to expose the foreign cells in Turkey.

Masharipov, the Reina nightclub attacker, said in his statement that he was sent to Turkey via Iran a year before the attack. He illegally crossed the border with his family and waited as a sleeper in Konya before being activated through orders sent from Raqqa. His emir in Raqqa provided weapons and hideout connections. When looking at Masharipov's connections in Turkey before the attack, it is clear that all were foreigners — an indication of the strict separation of Turkish and foreign cells in Turkey, aimed to ensure the security of its networks by preventing leaks and ensuring the cells cannot knowingly or unknowingly reveal each other's identities. It is also essential to understand that foreign fighters traveling through Turkey are not associated with any unrelated ISIS cell members; their passage is arranged by cells designated specifically for that purpose. These facilitating cells include both Turkish and foreign members who speak the language of the foreign fighters being transferred. Most of the time, these foreign fighters are asked to travel to border cities unless there are reasons for them to spend time in Turkey. They usually do not travel with other ISIS members and only meet with the designated ISIS members when necessary or when crossing borders illegally.

CONCLUSION

ISIS is a real threat to Turkey, Europe and the surrounding regions. The seriousness of this threat, with the ongoing political turmoil in Turkey, must be evaluated, especially considering that Turkey, a NATO country, has recently been forging closer ties with Russia. The risk of Turkey becoming a safe haven for terrorists cannot be dismissed, particulary when Turkey has suffered a considerable loss of its counterterrorism capacity and a 400 percent surge in terrorist attacks in recent years. Some of the former ISIS members interviewed at the International Center for the Study of Violent Extremism openly stated that, after losing major territories such as Mosul and Raqqa, ISIS fighters would shave off their beards and cut their hair to blend into society and continue terrorist activities. In fact, Turkey is one of the main conduits for fighters to disperse after a major defeat because they can still cross the borders with the help of smugglers. Several former ISIS members also reported that ISIS assigns people to countries where they would not attract as much attention based on their nationalities.

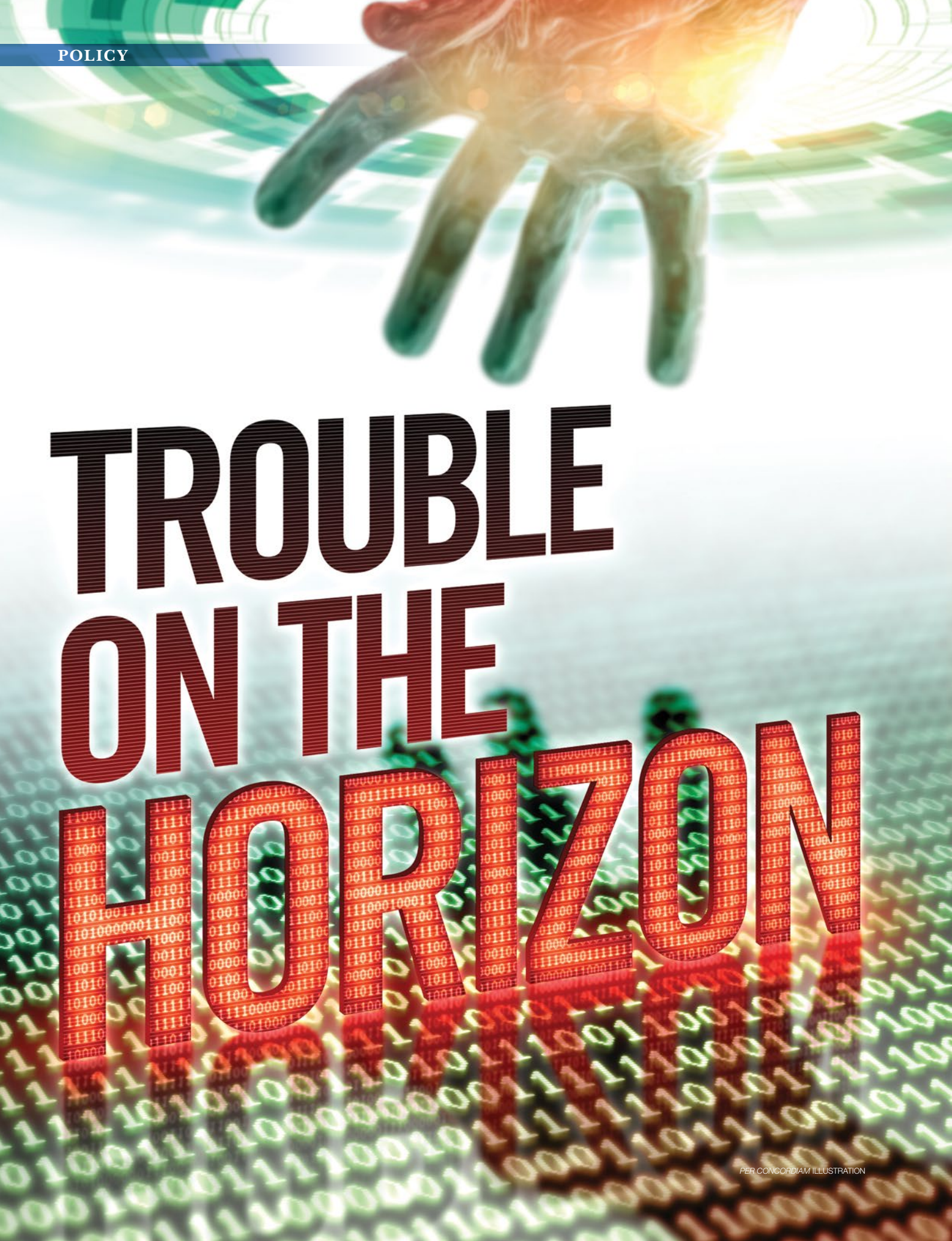
In light of this, Turkey is an attractive hub, currently hosting about 3 million Syrian refugees, and many Syrian ISIS members could easily hide among them. Even more alarming, based on the 2015 Pew Research survey, more than 6 million Turks out of a population of 78 million view ISIS favorably. While this number might have decreased due to recent attacks and the burning of two Turkish soldiers, it is obvious that the Turkish support base is vast and dispersed throughout the country, which enables ISIS to expect reliable support for future activities. While violent activity may be exclusive to cell members, it is essential to understand that the people who ideologically support ISIS in Turkey might be open to providing support and provisions, including financial and logistical support, hiding fugitives, or transporting weapons and fighters. Consequently, the existence of Turkish and foreign cells in Turkey and its vast support base for ISIS are major concerns not only for Turkey, but also for Europe, NATO and the U.S.

ISIS has been openly threatening Turkey as the al-Bab campaign continues. On February 3, 2017, ISIS asked its members in Turkey, through social media and Telegram chat channels, to carry out attacks against the police, military, tourists and Christians in the country, so it would be naive not to expect further attacks. Compounding the direct threat of ISIS attacks, Turkey has been going through a complicated crisis since the July 2016 coup attempt. It has lost more than 150,000 government officials, military personnel, police officers, judges and prosecutors. Over 90,000 officials were detained and almost 50,000 were arrested. The Turkish National Police experienced the largest setback, losing over 30,000 officers, including police chiefs and officers who spent years fighting terrorism. The Turkish military lost over half its active-duty generals and two-thirds of its F-16 pilots. And the judiciary was equally targeted, losing a third of its experienced prosecutors and judges across the country.

These purges and arrests have had significantly negative consequences. Turkey has lost its most experienced and well-trained people, as well as a great deal of wisdom in the fight against terrorism. All of these counterterrorism and intelligence officials were replaced with new officers who have no experience or training in counterterrorism. While this doesn't mean that the newly appointed officers will not try to fight terrorism, it is a bitter fact that it will take years for the Turkish National Police and the Turkish military to regain the capacity and experience they had before the coup attempt and corruption investigations triggered the purge. The lost capacity will result in the loss of innocent lives and will put additional strain on European countries and the U.S. because Turkey's ability to prevent the movement of terrorists across its borders has been degraded.

Winning the war against ISIS in Syria and Iraq will not completely dismantle it. While it will certainly diminish its capacity, it might also cause a surge of attacks or unrest in neighboring countries first and then in the rest of the world. We must not forget that terrorist organizations are very patient; as with the Reina nightclub attacker, sleeper cells can be inactive for years without detection, making it possible for terrorist organizations to carry out surprise attacks. Target-hardening and prevention measures should be re-evaluated to make it harder for terrorists to carry out attacks. It is essential to acknowledge that Turkey is a potential gateway for foreign terrorists, especially ISIS, and Turkey's success or failure in fighting terrorism is directly related to the security of the West and even the U.S. A diminished counterterrorism capacity in Turkey will result in more terror attacks in the West and chaos in the region. □

Ahmet S. Yayla is an adjunct professor of criminology, law and society at George Mason University in the United States. He formerly served as a professor and chair of the sociology department at Harran University in Turkey and as chief of the counterterrorism and operations department of the Turkish National Police in Sanliurfa. He is co-author of the book, *ISIS Defectors: Inside Stories of the Terrorist Caliphate.*



PER CONCORDIAM ILLUSTRATION

A looming cyber warfare threat demands an overhaul of international law

By Lt. Col. Brian Smith, U.S. Central Command
PHOTOS BY THE ASSOCIATED PRESS

Although some progress has been made over the past decade, current international law governing cyber warfare remains vastly inadequate. It is rife with ambiguity, fails to provide legal grounds for proportional retaliation in catastrophic scenarios, and fosters an international environment in which states feel no compulsion to treat cyber warfare as "warfare." As Sean D. Murphy notes in his 2012 book *Principles of International Law*, since the creation of Article 2(4) of the United Nations Charter, the International Court of Justice (ICJ), politicians and international law scholars have grappled with determining what exactly constitutes "use of force" and, therefore, what constitutes *jus ad bellum* (right to war). Also, the meaning of the term "use of force" is debatable; the U.N. General Assembly's 1974 resolution defining aggression failed to address many of the types of actions that might be deemed unlawful uses of force. Furthermore, what constitutes the right of self-defense, as outlined in the U.N.'s Article 51, has likewise been highly debated.

With the rapid increase in hacking in recent years, the need to address cyber warfare in explicit detail remains urgent. The failure to do so will eventually become catastrophic. In his 2014 book *Cybercrime and Cyberwarfare*, Igor Bernik finds that cyber warfare unfortunately fails to garner the attention it deserves within the international community. The U.N., NATO and other international organizations have faced cyber attacks on numerous occasions over the past decade, as noted by Nils Melzer in a 2011 paper, "Cyberwarfare and International Law." But none of the incidents led to significant change in international law, primarily because none of the incidents led to tragedy. That would change, however, with an attack resulting in a large number of casualties and billions in property damage.

Legal ambiguities

Cyber warfare is quickly becoming one of the leading global threats to industrialized nations. Yet the international law surrounding the threat remains rife with ambiguity. According to Murphy, at the center of this ambiguity are three critical questions. First, does a cyber attack constitute a use of force in violation of Article 2(4)? Second, does Article 51 allow a state to engage in cyber warfare pre-emptively? Third, should nonstate actors who conduct cyber warfare be treated the same as state actors? Sadly, investigations and legal maneuvers in the wake of cyber attacks in recent years have done little to address the ambiguity.

Although deliberations by the U.N. General Assembly and subsequent rulings by the ICJ support the conclusion that a cyber attack constitutes a use of force in violation of Article 2(4), this conclusion still comes with a degree of ambiguity. The General Assembly's 1974 "Definition of Aggression," published in Resolution 3314, defines aggression as the "use of armed force by a State" and provides a list of acts that qualify as aggression. In six of the seven acts, the term "armed forces" is reiterated, thus reinforcing its importance. Unfortunately, the term itself is not well-defined and the list of acts provided is remarkably small. Furthermore, in the first act listed, an "attack by the armed forces of a State," the word "attack" is not defined, according to Steven R. Ratner in his 2002 paper in the *American Journal of International Law*. Adding to the ambiguity, the Definition of Aggression also states that the list of acts is not exhaustive and that the U.N. Security Council may add to it.

Ratner also states that, despite the lack of clarity, Resolution 3314 confirms the understanding that aggression includes a variety of acts, and ICJ cases decided since the Definition of Aggression was published conclude that cyber attacks constitute a use of force. In the 1986 decision Nicaragua v. United States, the ICJ stated that sending armed bands amounts to an armed attack only if "because of its scale and effects" it serves as something more than a "mere frontier incident." This decision afforded states the opportunity to declare other states as aggressors even when the actions in question clearly fail to fall within the purview of the Definition of Aggression. As J. Martin Rochester noted in his 2006 book, *Between Peril and Promise: The Politics of International Law*, interstate war, particularly over territory, has become a "relatively peripheral concern" and remarkably infrequent. However, this uplifting fact is offset by the

reality that acts and threats of violence remain prevalent across the world, only in more complex forms more difficult to legally grasp. Rochester further states that the decline of interstate war as a ubiquitous norm of international relations has given way to what the Prussian military theorist Carl Von Clausewitz called "war by other means." The ability of international law to specifically label new forms of aggression as such is becoming more tenuous with each passing decade. The rapid evolution of cyber warfare, and whether a cyber attack constitutes a use of force in violation of Article 2(4), must be properly addressed if international laws governing cyber warfare are to advance and provide adequate legal recourse to victims.

Perhaps even more ambiguous than Article 2(4) and the use of force, is whether Article 51 allows a state to engage in cyber warfare pre-emptively, a question hotly debated in the international community. Marco Roscini, in his 2014 book, *Cyber Operations and the Use of Force in International Law*, argues that under Article 51, a state targeted by a cyber operation may only claim self-defense and react forcibly if the operation amounts to an "armed attack." He further notes that such an attack applies not only to traditional weapons, but also to "one with cyber means," provided that the extent of the attack amounts to a use of force under Article 2(4). This was reinforced by the 2004 opinion of the U.N.'s High-Level Panel on Threats, Challenges and Change, which appeared to support the loosening of the strict prerequisite of an "armed attack" as the only justification for a forcible reaction, according to a 2006 article by W. Michael Reisman and Andrea Armstrong in the *American Journal of International Law*. Providing a contrary opinion, Reisman and Armstrong argue that whether wise or not, Article 51 was not written to accommodate even the Caroline principle, considered by many international law scholars to be the standard for establishing a pre-emptive self-defense claim of any kind. Furthermore, they point out that in a series of judgments and advisory opinions, the ICJ held firmly to a strict reading of Article 51, concluding that a state's right to claim self-defense is subject to it "having been the victim of an armed attack."

Regarding the third question at the center of cyber law ambiguity — should nonstate actors who conduct cyber warfare be treated the same as state actors? — the U.N. Charter once again fails to provide clear legislation for the domain of cyber warfare. Richard A. Clarke and Robert K. Knake, in their 2010 book *Cyber War: The Next Threat to National Security and What to Do About It*, define cyber warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." Their use of the term "nation-state" undoubtedly stems from the recurring use of the word "state" within Resolution 3314. As Bernik also finds, the lack of specific universal definitions and the lack of consensus on the definition of key concepts alone indicates that cyber criminals continue to stay ahead in the fight. The continued use of the word "state" in Article 2(4) and the failure of international law to distinguish properly between the actions of state and nonstate actors adds to the ambiguity of cyber warfare. This failure turns the debate into a war of semantics, similar to the debate surrounding the invasion of Iraq in 2003. As Curtis A. Bradley and Jack L. Goldsmith noted in their 2005 *Harvard Law Review* article, many times prior to 2003, U.S. presidents initiated hostilities without congressional authorization, even when, arguably, in violation of the U.N. Charter.

Shaky legal ground

Current international law fails to prevent or discourage the use of force within the cyber domain because it fails to provide legal grounds for proportional retaliation in catastrophic scenarios. In a world increasingly dominated by cyberspace, the need for appropriate cyber warfare legislation is becoming more urgent. Unfortunately, as Jack L. Goldsmith and Eric A. Posner remark in a 1999 University of Chicago Law School article, *opinio juris*, legality, morality and similar concepts mean little to states on the international stage, and one could argue that they mean much less to the primary actors of the cyber domain. Most cyber actors will never comply with the norms of international law out of a sense a moral or legal obligation. They will comply when it's in their own states' interests. Further, Jason D. Jolley writes in his paper, published in the Canadian Center of Science and Education journal *International Law Research* in 2013, that without adequate legislation prohibiting cyber warfare, states will continue to disregard international norms and utilize their technological expertise to unleash cyber attacks. As long as states can argue that their actions do not violate international law, they will continue to exploit other states' weaknesses for economic, political or military advantage, resulting in a continuous escalation of nefarious acts to the point where large-scale tragedy becomes inevitable.

To understand the seriousness of cyber warfare and the inadequacy of international cyber warfare legislation, one must take a hard look at what cyber actors are capable of and the legal options available to their potential victims. Clarke and Knake warn that cyber attacks have the potential to cause airplanes to crash, trains to derail, chemical plants to release poisonous gas, gas pipelines to explode, enemy units to walk into ambushes and much more. In this doomsday scenario, a sophisticated cyber attack on America's infrastructure cripples the most advanced nation on the planet in a mere 15 minutes and causes the deaths of thousands of people. Such a massive and coordinated attack seems highly implausible, but to test the limits of current cyber warfare legislation, one need only consider the consequences of just one of these tragic events.

One scenario involves hackers infiltrating a nuclear power plant and causing a power surge, which triggers an attempted emergency shutdown, a much larger subsequent spike in power output and eventually a reactor vessel rupture. Following the rupture, a series of steam explosions exposes the internal structure of the reactor to air, causing it to ignite. The resulting fire sends radioactive fallout into the atmosphere, which then lands and contaminates millions of acres and those living on it. The immediate death toll is in the dozens, but the expected long-term death toll reaches the thousands. As unlikely as the scenario may sound, the two critical events

German Interior Minister Thomas de Maiziere stands before a map in February 2017 that illustrates the number of cyber attacks in Europe over a 30-day period.

of this scenario have already played out in real-world events, according to Jolley. In 2010, a malicious software virus named "Stuxnet" caused as many as 2,000 centrifuges at an Iranian nuclear power plant to change speeds rapidly, inducing vibrations that destroyed the centrifuges. In 1986, the Chernobyl Nuclear Power Plant suffered an unexpected power surge that resulted in radioactive fallout.

There is nothing preventing a virus like Stuxnet from being used to cause the type of accident that occurred in Chernobyl. And when an event of this magnitude eventually does take place, according to Paul Rosenzweig's 2013 book *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World*, the international community will undoubtedly realize that existing international legislation fails to address such an attack. In addition, long-standing assumptions and frameworks for settling conflict will disappear, seemingly overnight, and how states fight wars will have to be rethought, as will the definitions of armed attack, terrorism, espionage and crime. The atomic bombings of Hiroshima and Nagasaki were the last time the international community was forced to examine the limits of international law so carefully. Although Stuxnet caused nowhere near the same level of destruction, Rosenzweig writes that the "cognitive disruptions that will come are just as great" and that the virus was, figuratively, just the first explosion of a cyber atomic bomb.

When investigating the future of cyber warfare and the potential devastation that lies ahead, Jolley reminds us it is critical to remember how electronically interconnected states are and how much cyberspace dominates the world. An enormous portion of our lives is controlled by computer systems and networks, from utilities to shopping and from banking to social interactions. Critical infrastructure depends almost completely on computer systems and networks to control everything from commercial transportation to water purification, to communications and much more. Because of our dependence on cyberspace, Jolley states, we must re-evaluate the definition of the "use of force" and how to test for it. In short, the international community must rewrite the rules of cyber warfare and establish a multilateral treaty prohibiting the "use of force" in the cyber domain.

International indifference

Despite large-scale cyber attacks over the past decade, the international community continues to muddle along without legislation capable of dealing with cyber warfare. As Bernik remarked, "outdated, rigid, and fragmented legislation"

A French police officer works at a state-sponsored facility that investigates cyber crimes reported by the public.

prevents the development of physical and legal safeguards to cyber warfare by competent authorities and prevents the proper courses of action being taken by victims of cyber attacks. At the heart of the issue lies a pervasive mood of general indifference, which owes its existence to a variety of more specific issues. First, the international community's overall knowledge of the cyber warfare threat remains remarkably limited. Second, a viable approach for developing adequate cyber warfare legislation appears elusive. Third, even if adequate legislation did exist, the perpetrators of cyber warfare display far less respect for international law than those fighting against them, making compliance difficult to achieve. Unlike the typical actors in past interstate wars who held at least some regard for their standing within the international community, today's typical cyber warrior is often nothing more than a small terrorist or political organization with no concern for international law. The lack of knowledge can and almost certainly will be fixed over time, if only in the aftermath of tragedy; however, the demographics surrounding cyber warfare make the third issue far more problematic than the first two.

Improving cyber warfare legislation won't happen until the international community fully understands the threat. Fortunately, as Stephen D. Krasner notes in his 1982 article in the journal *International Organization*, history shows that increased knowledge plays an invaluable role in revolutionizing politics and states' behavior, especially in areas such as public health and arms control. For example, the explosion of global scientific knowledge in the mid-20th century radically altered rules governing the use of vaccines. Prior to the explosion, national health regulations regarding vaccines were dictated by politicians with no medical knowledge, but afterward national policies were influenced by an international regime. The same held true with the arms race. The realization of mutual assured destruction (MAD) by both the U.S. and the Soviet Union provided a basis for a regime. Without both sides knowing the reality of MAD, knowledge would have had no impact on regime development. Ironically, cyber warfare appears to be developing into a new type of arms race and, hopefully, the international community will respond with appropriate legislation before tragic events unfold.

In addition to the lack of awareness of the cyber warfare threat, the international community also lacks a viable approach for developing adequate legislation. On opposing sides of the fight are realists, who believe that institutions play a minimalist role in influencing state behavior, and liberal institutionalists, who believe that institutions are the key to influencing state behavior. In his 1994 article, "The False Promise of International Institutions," John J. Mearsheimer argued that the international system is anarchic and institutions are little more than a reflection of the balance of power in the world. He further remarked that many policymakers naively believe that institutions hold great promise for creating international peace. Considering the present anarchic nature of the cyber world, where actors operate largely in the shadows and their actions are difficult to trace and nearly impossible to prosecute, Mearsheimer's view appears to hold water in cyberspace. At all levels, cyber actors "look for opportunities to take advantage of each other," and at the state level actors strive not only to achieve cyber hegemony but also to prevent other actors from achieving the same lofty position. An offensive realist such as Mearsheimer would likely argue that a powerful state actor in the cyber domain would be wise to attempt to achieve hegemonic status before others do, especially considering that if executed properly, such a status could be achieved before the rest of the actors even realized it. Nevertheless, from the present and impersonal state of the cyber domain, it is easy to see why many actors feel frustrated by the failure of institutions to achieve peace and order and, hence, why indifference runs rampant.

Taking a more optimistic approach, institutionalists argue that it is not necessary to develop cyber warfare legislation under the backdrop of a doomsday scenario, such as that proposed by Clarke and Knake, and that the vast majority of international laws exist to control state behavior in very benign circumstances. Despite the widespread opinion of cyber experts that it's only a matter of time before a large-scale cyber attack takes place with tragic consequences, few believe that cyber warfare is an existential issue for states. In 2004, Detlev F. Vagts analyzed the Goldsmith-Posner view on customary law and noted in his essay in the *European Journal of International Law* that customary law is strongest when "the

costs of compliance are not enormous." By this, Vagts simply implies that there are many laws that don't directly deal with the life and death of the state, and those laws are important, too. Cyber laws will become more critical to the international community with every passing year, but they will never be about state survival. With this in mind, it is important to realize that some success in cyber legislation is better than no success at all. Myres S. McDougal, in the 1952 article "Law and Power," wisely notes that people who truly strive to avoid violence, except in self-defense or organized community sanction, have only the alternative of some type of law, whether domestic or international. This is especially true of countries incapable of defending themselves against much more powerful belligerents. He continues by arguing that the choice cannot be between law and no law, but rather between effective and ineffective law. John Gerard Ruggie summarized the realist approach in his 1995 paper, "The False Premise of Realism." Noting that, however weak institutions might be today, even minimal contributions of peacekeeping and nonproliferation are better than nothing.

Perhaps the greatest cause of indifference and, simultaneously, the greatest threat to any future cyber warfare legislation is the perceived potential of noncompliance. Given the extraordinary nature of cyber warfare and the rate of its evolution, past theories on why states obey international law may not apply to this domain. In their 2012 paper, "Constructivism and International Law," Jutta Brunnée and Stephen J. Toope argue that law becomes persuasive when the relevant actors view it as legitimate, especially when it inspires reasoned argument to justify its processes. This view is supported by Thomas M. Franck in a 1988 article in the *American Journal of International Law*, but he adds that "in a community organized around rules, compliance is secured — to whatever degree it is — at least in part by perception of a rule." Here, Franck implies that legitimacy of legislation as a solution for state compliance is only guaranteed to be applicable in a community that already respects rules. For terrorist organizations or states that sponsor or support terrorism, such as North Korea and Iran, legitimacy of cyber warfare legislation means almost nothing because such entities have little or no respect for rules or regimes. Furthermore, the Franck fairness model holds little promise for compliance in a domain where it is difficult to obtain the evidence needed to prosecute violations of law.

Adding to the potential for noncompliance, the cyber warfare domain does not benefit from standard constructivist tools that further the development of international law in other domains. As Brunnée and Toope noted, actors "learn" through patterns of interaction to read the social environment in which norms are shaped and influenced. Unfortunately, the primary actors in the cyber domain, or at least those that "first world" states are most concerned about, are typically actors who have little or no meaningful interaction with those that they target. Cyber criminals, from the lone hacker in a basement to a state-sponsored group in China, do not socially interact with others on an international stage or in ways that foster the development of appropriate cyber law. Furthermore, as Brunnée and Toope argue, the social interaction needed to further the development of cyber law is only effective when most of the actors involved believe that most others will understand the laws the same way they do and comply in the same way. Such would not be the case in the cyber domain.

Leading theorists of international law provide a wide variety of reasons for the international community's indifference to cyber warfare law. Ultimately, as Harold Koh noted in his 1997 article "Why Do Nations Obey International Law?" no one theory can explain the behavior of all states all of the time, and thus, the only way to determine what will make cyber warfare actors comply is a thorough analysis of all reasonable theories, drawing from them the characteristics that appear most applicable.

Conclusion

The world has not yet witnessed dramatic humanitarian consequences as a result of cyber warfare but, as Melzer points out, the potential for human tragedy is enormous and increases every year as our lives become more and more dependent on computer-controlled systems. As far as international law is concerned, cyber warfare does not exist in a vacuum, but it has not been given the attention it deserves. To deter large-scale cyber attacks and prevent smaller attacks from escalating into larger ones, the international community must begin to transpose existing rules and principles to the relatively new domain of cyber warfare. New treaties must be forged and existing definitions must be changed. Doing so will be difficult because the international community is largely uneducated in cyber warfare, the technologies within the cyber domain change so rapidly, and many of the key actors in the domain are unidentifiable and uninterested in changing the rules.

From a theoretical standpoint, it is difficult to gauge whether new international laws will see greater success from a realist or institutionalist perspective. Realists focus primarily on the international-system level of analysis and dismiss the importance or impact of the individual and the nature of the state in the decision-making process. Therefore, realists and neorealists such as Mearsheimer would likely argue to leave institutions such as the U.N. and NATO out of the picture. Such a perspective is convenient for citizens of the most powerful state in the world, but it wouldn't sit well with smaller states, such as Estonia, which depends on international institutions for protection and in 2007 suffered the largest cyber attack to date at the hands of neighboring Russia. On the other hand, realists consider states to be a group of introverts incapable of rational dialogue and suspicious of every foreign move, and such a description is very applicable to many of the primary actors in cyber warfare. Regardless, due to the uncertainty that lies ahead in the cyber domain, some action is better than no action at all and it is time for the international community to rewrite the rules of cyber warfare. As the Dutch jurist Hugo Grotius brilliantly remarked, "All things are uncertain the moment men depart from law." □

ON THE OFFENSIVE

ARGENTINA'S MULTIPRONGED ASSAULT ON DRUG TRAFFICKING PROVIDES LESSONS FOR OTHER NATIONS

BY MARTIN VERRIER

Argentina's national undersecretary of
Counter Narcotics Policy, Marshall Center Alumni

Drug consumption in Argentina skyrocketed during the first decade of this century. Marijuana use nearly doubled between 2004 and 2010, while cocaine use by the general population rose from about 0.3 percent in 2004 to 1 percent in 2010, according to a government report.

This increase in consumption has changed Argentina's role in transnational drug trafficking. Formerly known as a transit country for cocaine heading mainly toward Europe by ship, drugs are now smuggled across the border by land and by air. Cocaine from Bolivia and Peru is smuggled aboard illegal flights into the country or dropped from aircraft within Argentina's borders. Some of this cocaine is consumed locally while higher quality cocaine is smuggled to its final destination in Europe or Chile.

Marijuana is trafficked from Paraguay, one of South America's biggest cannabis producers. Marijuana shipments are often trafficked along fast-flowing rivers, such as the Parana, connecting Argentina with Paraguay, Brazil and Uruguay.

THE FIGHT AGAINST DRUGS BECAME A PRIORITY, MEANING A NEW STRATEGY WAS NEEDED TO FACE THE THREAT.

In recent years, synthetic drugs such as Ecstasy and methamphetamine have made an explosive appearance in Argentina, especially in the numerous dance clubs in Buenos Aires. Most of these drugs come from European countries, such as the Netherlands and Germany, and are trafficked mainly through commercial airline flights and private couriers.

The previous government administration never enacted a coherent strategy to face this growing problem. Only isolated measures were taken, such as increasing personnel and temporary force redeployments (Argentina has four federal forces: Gendarmeria Nacional, Prefectura Naval, Policia Federal and Policia de Seguridad Aeroportuaria). Public officials and decision-makers were in a state of denial — to them, drugs were not a problem for Argentina.

NEW PRIORITIES

In December 2015, a new administration, led by Mauricio Macri, was elected to end 12 years of "Kirchnerismo" (Nestor Kirchner ruled from 2003 to 2007, followed by his wife from 2007 to 2015). The fight against drugs became a priority, meaning a new strategy was needed to face the threat.

The first challenge was to understand the seriousness of the drug trafficking situation. Federal forces were given a standard form to complete after every drug operation that pinpointed where the activities took place. As a result, a map depicting drug operations across the country is now maintained and continually updated at the office of Counter Narcotics Policy.

The second challenge was to identify a strategy for combating the trafficking. In doing so, it was discovered that the best way to understand how organized crime operates, and consequently neutralize the activity, is to follow a strategy developed by criminologist Jay Albanese. In his 2011 book, *Transnational Crime and the 21st Century*, Albanese states that four factors have an impact on how freely organized crime operates:

- The behavior of supply.
- The behavior of demand (the customers).
- The behavior of regulators (the business environment).
- The behavior of competition (affecting profits).

A FRESH APPROACH

The Ministry of Security decided to introduce a strategy based on these four pillars. First, concerning supply, the following actions were taken: enhanced use of criminal intelligence to monitor groups and organizations operating at the border; tightened border controls; increased use of military 3-D radars at the border; increased control over chemical precursors (more than 1,000 industries where supervised); creation of a new office overseeing border affairs; and agreements for common operations with neighboring countries. Also important was the creation of two task forces, one in the northwest (with support from the United States) and one in Buenos Aires' main airport, Ezeiza, under the United Nations Office on Drugs and Crime's (UNODC's) Airport Communications Program (AIRCOP). Both represent transformative innovation for Argentina's domestic security structure.

The number of officers with special drug training was increased by 168 percent. Moreover, four border hot spots will be patrolled by a new electronic surveillance system, and four speedboats will patrol the rivers. A joint operation among Argentina, Paraguay and Brazil in the tri-border area was launched in February 2016, and five regional fusion centers were established by the National Directorate of Criminal Intelligence to share criminal information from the provinces with federal forces.

Another important decision was to redeploy the Federal Police under true federal criteria, creating eight regional offices and 29 narcotics offices. Previously, this agency had most of its resources concentrated in Buenos Aires.

Second, regarding demand, the main drug prevention and treatment agency, La Secretaría de Políticas Integrales sobre Drogas, or SEDRONAR, implemented a renewed strategy for drug treatment focused on the local or municipal level. Moreover, increased supply control is driving up prices. This is the case for coca leaf, with a 20 percent price increase this year. Based on different research papers, it is assumed that an increase in price will lead to a decrease in consumption.

Third, regarding the regulatory environment, a huge effort has been made to enact legislation.

Argentine officials seize over 4,000 litres of chlorhydric and sulfuric acid in September 2016. The chemicals are used to prepare cocaine for sale.
ARGENTINE MINISTRY OF SECURITY

A new law targets precursors, the substances that can be used to make illicit drugs. A list of prohibited drugs was introduced and a new law created that groups any drugs under common molecular families with an "analog" criteria. Enhancing international cooperation was also a priority. Argentina signed cooperation agreements with Bolivia, Paraguay, the U.S., Russia, China, Israel and Germany, among others, that incorporated all UNODC early warning systems, such as the Precursor Incident Communication System, the Early Warning Advisory program and AIRCOP.

Finally, regarding profitability, a plan was introduced reforming how Argentina's Financial Action Office works. In early 2016, the local office was again accepted by the U.S. Treasury Department's Financial Crimes Enforcement Network. The U.S. Drug Enforcement Agency trained federal forces and prosecutors on money laundering investigations. Several drugs lords saw their assets frozen because of criminal investigations, and some of those assets were seized and given to federal agencies.

These are only some of the actions taken for each of the pillars that support the new general strategy. Much work still needs to be done, but indicators for this year are encouraging. During the first year of the current administration, while marijuana seizures remained stable, cocaine seizures rose by 28 percent, coca leaves by 4 percent and synthetic drugs by 512 percent. This increase in seizures was driven by an increase in anti-drug operations, which rose by 7 percent, and by focusing on larger organizations (detainees decreased by 7 percent, proving that fewer consumers and small traffickers were targeted). Regarding chemical precursors, a third more establishments were inspected compared to the previous year. □

Resident Courses

Democratia per fidem et concordiam
Democracy through trust and friendship

Registrar
George C. Marshall European Center
for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
Telephone: +49-8821-750-2327/2229/2568
Fax: +49-8821-750-2650

www.marshallcenter.org
registrar@marshallcenter.org

Admission
The George C. Marshall European Center for Security Studies cannot accept direct nominations. Nominations for all programs must reach the center through the appropriate ministry and the U.S. or German embassy in the nominee's country. However, the registrar can help applicants start the process. For help, email requests to: registrar@marshallcenter.org

PROGRAM ON APPLIED SECURITY STUDIES (PASS)

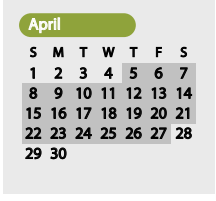
The Marshall Center's flagship resident program provides graduate-level education in security policy, defense affairs, international relations and related topics such as international law and counterterrorism. A theme addressed throughout the program is the need for international, interagency and interdisciplinary cooperation.

PASS 17-15
Sept. 6 -
Nov. 16, 2017

PROGRAM ON COUNTERING TRANSNATIONAL ORGANIZED CRIME (CTOC)

This two-week resident program focuses on the national security threats posed by illicit trafficking and other criminal activities. The course is designed for government and state officials and practitioners who are engaged in policy development, law enforcement, intelligence and interdiction activities.

CTOC 18-07
Apr. 5 - 27, 2018

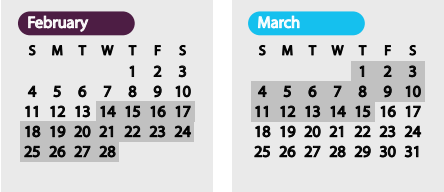


CTOC 18-14
Aug. 2 - 24, 2018

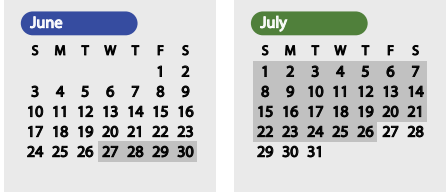
PROGRAM ON TERRORISM AND SECURITY STUDIES (PTSS)

This four-week program is designed for government officials and military officers employed in midlevel and upper-level management of counterterrorism organizations and will provide instruction on both the nature and magnitude of today's terrorism threat. The program improves participants' ability to counter terrorism's regional implications by providing a common framework of knowledge and understanding that will enable national security officials to cooperate at an international level.

PTSS 18-05
Feb. 14 -
Mar. 15, 2018



PTSS 18-12
June 27 -
July 26, 2018



PROGRAM ON CYBER SECURITY STUDIES (PCSS)

The PCSS focuses on ways to address challenges in the cyber environment while adhering to fundamental values of democratic society. This nontechnical program helps participants appreciate the nature of today's threats.

PCSS 18-02
Dec. 5 - 21, 2017

December

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

SEMINAR ON REGIONAL SECURITY (SRS)

The three-week seminar aims at systematically analyzing the character of the selected crises, the impact of regional actors, as well as the effects of international assistance measures.

SRS 18-04
Jan. 18 -
Feb. 8, 2018

January

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

February

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28			

SENIOR EXECUTIVE SEMINAR (SES)

This intensive five-day seminar focuses on new topics of key global interest that will generate new perspectives, ideas and cooperative discussions and possible solutions. Participants include general officers, senior diplomats, ambassadors, ministers, deputy ministers and parliamentarians. The SES includes formal presentations by senior officials and recognized experts followed by in-depth discussions in seminar groups.

SES 18-11
June 4 - 8, 2018

June

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Alumni Programs

Dean Reed
Director, Alumni Programs
Tel +49-(0)8821-750-2112
reeddg@marshallcenter.org

Alumni Relations Specialists:

Barbara Wither
Southeast Europe
Languages: English, Russian, German, French
Tel +49-(0)8821-750-2291
witherb@marshallcenter.org

Christian Eder
Western Europe
Languages: German, English
Tel +49-(0)8821-750-2814
christian.eder@marshallcenter.org

Marc Johnson
Central Asia, South Caucasus, Russia, Moldova, Ukraine, Belarus - Cyber Alumni Specialist
Languages: English, Russian, French
Tel +49-(0)8821-750-2014
marc.johnson@marshallcenter.org

Christopher Burelli
Central Europe, Baltic States - Counterterrorism Alumni Specialist
Languages: English, Slovak, Italian, German
Tel +49-(0)8821-750-2706
christopher.burelli@marshallcenter.org

Donna Janca
Africa, Middle East, Southern and Southeast Asia, North and South America - CTOC Alumni Specialist
Languages: English, German
Tel +49-(0)8821-750-2689
nadonya.janca@marshallcenter.org

mcalumni@marshallcenter.org

Contribute

Interested in submitting materials for publication in *per Concordiam* magazine? Submission guidelines are at **http://tinyurl.com/per-concordiam-submissions**

Subscribe

For more details, or a **FREE** subscription to *per Concordiam* magazine, please contact us at **editor@perconcordiam.org**

Find us

Find *per Concordiam* online at:
Marshall Center: **www.marshallcenter.org**
Twitter: **www.twitter.com/per_concordiam**
Facebook: **www.facebook.com/perconcordiam**
GlobalNET Portal: **https://members.marshallcenter.org**
Digital version: **http://perconcordiam.com**

The George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany

MARSHALL CENTER