AMERICANBARASSOCIATION
Rule of Law Initiative

UKRAINE INTERNET FREEDOM PROGRAM

THE POLITICAL LANDSCAPE IN PERSPECTIVE

In a perilous political landscape, we will explore the expanding space for internet freedom in Ukraine. Our goal is to provide a balanced perspective on the threats to protection of cyberspace, freedom of speech and expression, data protection, privacy and fundamental human rights.

ABA ROLI'S GOAL

It is in this context that the ABA Rule of Law Initiative seeks to advance laws and policies that promote internet freedom, freedom of expression online, and transparency, as well as strengthen the protection of human rights online against violations.

THE CORE QUESTION

This is the core question we will address in today's program:

“SHOULD UKRAINE DEVELOP INTERNATIONAL AGREEMENTS ON THE PROTECTION OF PERSONAL DATA RELATED TO THE PREVENTION, INVESTIGATION, DETECTION, AND PROSECUTION OF CRIMINAL OFFENSES, USING COMPARABLE USA/EU AGREEMENTS AS A MODEL?”

INVITED SPEAKER: BENJAMIN E. GRIFFITH

Date: 15 February 2022

Time: 15:00-19:00 Kyiv time, Ukraine (08.00 AM 12.00 PM, EST)

Language: English and Ukrainian with simultaneous translation

Format: Online (Zoom)

The event is free, but requires pre-registration, to register, please follow the link

UMBRELLA AGREEMENT

In 2016, the US and European Union signed an Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, better known as the “Umbrella Agreement.” The purpose of this Agreement is to ensure a high level of protection of personal information and enhance cooperation between the United States and the European Union and its Member States, in relation to the prevention, investigation, detection or prosecution of criminal offences, including terrorism. For this purpose, the Agreement established the framework for the protection of personal information when transferred between the United States, on the one hand, and the European Union or its Member States, on the other.

INTERNATIONAL COOPERATION

Within the framework of digitalization efforts, the Ukrainian government is looking for ways to become more responsive to international cooperation in crime prevention and personal data protection. With this regard, the government is looking for opportunities and possibilities to start negotiating similar opportunities for multinational personal data protection agreements.

PURPOSE OF UKRAINE INTERNET FREEDOM PROGRAM

The purpose of this event is to start discussing personal data protection in Ukraine, considering the US and the EU experience, while seeking opportunities to join the international data protection movement after modernizing the Ukrainian legal framework.

The following topics will be covered and discussed during this event:

I. CURBING MALICIOUS ACTITIES & MALIGN ACTORS

Organized crime and State-Sponsored Criminal Corruption :

- **UNCAC:** *United Nations Convention Against Corruption,* U.N. Office on Drugs and Crime, United Nations, New York 2004

  The United Nations Convention against Corruption is the only legally binding universal anti-corruption instrument. It was adopted by the UN General Assembly 31 October 2003, by resolution 58/4. It entered into force 14 December 2005, in accordance with article 68(1), and had 140

Signatories. The adoption of UNCAC was intended to warn the corrupt that betrayal of the public trust will not be tolerated, and it reaffirms the importance of core values such as honesty, respect for the rule of law, accountability and transparency in promoting development and making the world a better place for all.

UNCAC'S COMPREHENSIVE RESPONSE

As the only legally binding universal anti-corruption instrument, the Convention (also referred to as UNCAC) has a far-reaching approach, and the mandatory character of many of its provisions make it a unique tool for developing a comprehensive response to a global problem. The Convention covers five main areas:

1. preventive measures,
2. criminalization and law enforcement,
3. international cooperation,
4. asset recovery, and
5. technical assistance and information exchange.

FIGHTING CORRUPTION IN PUBLIC AND PRIVATE SECTORS

The comprehensive set of standards, measures and rules introduced by UNCAC are available for all countries to apply in order to strengthen their legal and regulatory regimes to fight corruption in both the public and the private sectors.

The Convention covers many different forms of corruption, such as bribery, trading in influence, abuse of functions, and various acts of corruption in the private sector. A highlight of the Convention is the inclusion of a specific chapter on asset recovery, aimed at returning assets to their rightful owners, including countries from which they had been taken illicitly. The vast majority of United Nations Member States are parties to the Convention.

NINTH CONFERENCE OF UNCAC

The 9th Conference of the States Parties to the United Nations Convention against Corruption was held in Egypt on December 13-17, 2021.

UNITED STATES STRATEGY ON COUNTERING CORRUPTION

Pursuant to the National Security Study Memorandum on Establishing the Fight Against Corruption as a Core United States National Security Interest (WH December 2021)

NSSM-1

On June 3, 2021, President Joe Biden established the fight against corruption as a core national security interest of the United States. In National Security Study Memorandum-1 (NSSM-1), he wrote "corruption threatens United States national security, economic equity, global anti-poverty and development efforts, and democracy itself.…[B]y effectively preventing and countering corruption and demonstrating the advantages of transparent and accountable governance, we can secure a critical advantage for the United States and other democracies."

In parallel with an interagency review by federal departments and agencies to assess existing U.S. Government anti-corruption efforts and identify persistent gaps in the fight against corruption, these efforts have been accelerated and amplified to prevent and combat corruption at home and abroad.

This first United States Strategy on Countering Corruption lays out a comprehensive approach for how the United States will work domestically and internationally, with governmental and non-governmental partners, to prevent, limit, and respond to corruption and related crimes. The Strategy places special emphasis on the transnational dimensions of the challenges posed by corruption, including by recognizing the ways in which corrupt actors have used the U.S. financial system and other rule-of-law based systems to launder their ill-gotten gains.

To curb corruption and its deleterious effects, the U.S. Government will organize its efforts around five mutually reinforcing pillars of work:

- Modernizing, coordinating, and resourcing U.S. Government efforts to fight corruption;
- Curbing illicit finance;
- Holding corrupt actors accountable;
- Preserving and strengthening the multilateral anti-corruption architecture; and,
- Improving diplomatic engagement and leveraging foreign assistance resources to advance policy goals.

To address the global reach of corruption and its pernicious effects, the U.S. will elevate and expand the scale of diplomatic engagement and foreign assistance, including the following:

(1) enhancing partner governments' capacities to fight corruption in cooperation with U.S. law enforcement authorities and bolstering the prevention and oversight capacities of willing governments.

(2) improving consistency and risk analysis across foreign assistance, ensuring joint analysis to better understand corrupt networks, the likely impact of U.S. assistance on corruption dynamics, and best practices for mitigating risk in particular contexts.

(3) Improving security assistance and integrating anti-corruption considerations into military planning, analysis, and operations and develop new protocols for assessing corruption risk.

(4) Tailoring diplomatic engagement and public diplomacy efforts to local conditions, elevating anti-corruption as a priority and supporting governmental and non-governmental actors combatting corruption through bilateral and multilateral contexts.

(5) Pursuing a substantial expansion in anti-corruption assistance, and will monitor the efficacy of this assistance, including through external evaluations.

(6) Integrating anti-corruption considerations across other spheres of development assistance, including global health, anti-crime and rule of law, conflict and fragility, and humanitarian assistance.

RULE OF LAW INITIATIVES ABROAD

In furtherance of the Rule of law initiatives abroad, the United States will establish new and expanded foreign assistance programs to enhance the capacity and independence of oversight and accountability institutions, including legislatures, supreme audit institutions, comptrollers, and inspector generals. Additional programs will strengthen the capacity of countries to "follow the money." These will supplement long-standing foreign assistance initiatives that strengthen public financial management, build justice sector institutions, and support e-governance and digitization, which can reduce opportunities for corruption.

INTERNATIONAL COOPERATION IN COMBATTING CORRUPTION

Ukraine considers IT tools to be the basis for effective fight against corruption and is ready to share with the international community its experience in implementing them. This was stated by Deputy Chairman of the National Agency for the Prevention of Corruption, Oleksandr Starodubtsev, at the 9th Conference of States Parties to the UN Convention against Corruption, according to the NAPC press service.

"We believe that international cooperation is vital to combating corruption, and we are ready not only to talk about our experience, but also to prove our commitment to the UN Convention. We are ready to share the code of these products and adapt it to the needs of your organization. To help you develop a user-friendly interface and provide you with effective design solutions," Starodubtsev said in an address to the countries participating in the Conference.

NAPC'S ANTI-CORRUPTION TOOLS: MODEL FOR UKRAINE?

Starodubtsev's speech was dedicated to six innovative anti-corruption tools applied by the NAPC, designed to create a new system of relations between the state and its citizens.

Among them are the Register of Declarations, the Register of Political Party Reports POLITDATA, the Anti-Corruption Portal, the Concealed Interests Portal, the Register of Corrupt Persons, and the Corruption Reporting Portal, which will soon be presented by the Agency. Oleksandr Starodubtsev spoke about the main technical characteristics of the said tools and the results of their implementation.

According to the deputy chairman of the NAPC, today the world economy depends on rapid transactions, mobile banking, and cryptocurrency. Crisis conditions such as COVID-19 affect the way people act and create more opportunities for corruption. Thus, anti-corruption bodies cannot maintain outdated approaches to tackling graft as long as offenders operate in the digital domain.

To address the issue, the Ukrainian delegation proposed that a dedicated platform be developed for the exchange of best digital practices and tools applied around the world, similar to that of Europol's cybercrime cooperation. Starodubtsev added that for truly effective cooperation in this area, it is especially important that all countries today share common data standards. In the future, this will facilitate data sharing and improve existing anti-corruption mechanism.

MICROSOFT DIGITAL DEFENSE REPORT

During the past year, 58% of all cyberattacks observed by Microsoft from nation-states have come from Russia. See *Microsoft Digital Defense Report*, October 2021, *infra*. Attacks from Russian nation-state actors are proving to be increasingly effective, increasing from a 21% successful compromise rate last year to a 32% rate this year. Russian nation-state actors are increasingly targeting government agencies for intelligence gathering, which jumped from 3% of their targets a year ago to 53% – largely agencies involved in foreign policy, national security or defense.

CYBERATTACK JANUARY 2022

Now jump to the second week of January 2022, when hackers temporarily shut down about 70 websites of Ukrainian national and regional government entities. The cyberattacks against Ukraine interrupted access to a series of government websites and left this message: "All your personal data has been uploaded, and data on this computer has been irrecoverably destroyed. All your information is now public. Be afraid and expect the worst." While no major damage was done, the SBU, Ukraine's Security Service reported that preliminary results of an investigation pointed to hacker groups linked to Russia's intelligence services responsible for hacking the infrastructure of a commercial company that had access with administrator privileges to affected websites. See *Ukraine Hacks Add to Worries of Cyber Conflict With Russia, infra.*

This series of cyberattacks added to escalating animosity and simmering tensions between Russia and Ukraine, converging at a time when

►an estimated 120,000 Russian troops are amassed on the border with Ukraine

►lethal U.S. military aid has begun arriving in Ukraine to help bolster Ukraine's defenses in the face of growing Russian aggression

►Vladimir Putin has demanded unilateral guarantees that would prevent Ukraine from ever joining NATO and require the NATO alliance to roll back its forces to the positions held in 1997 before Central and Eastern European nations joined NATO

►during a frenetic period of international activity with the U.S. publicly accusing Russia of either preparing a further invasion of Ukraine or of creating a pretext or a false flag operation to do so.

FREELANCERS OR STATE-BACKED ATTACKS?

While questions remain over whether the website attacks are simply the work of freelancers or part of a larger state-backed operation, and whether these attacks necessarily point to an imminent escalation by hostilities by Russia, some say this may well be Russia's next step in its aggression that began in 2014 with its forcibly taking the Crimean peninsula, preceded by Russia's cyber operations against Ukraine that entailed a hack of Ukraine's voting system before the 2014 national elections. Those hacks were followed by a hack of Ukraine's power grid in 2015 and 2016, then by the 2017 NotPetya cyberattacks which targeted Ukrainian businesses and caused over $10 billion in damage globally. See *Ukraine Hacks Add to Worries of Cyber Conflict With Russia,* Security Week/AP January 14, 2022.

https://s1.securityweek.com/ukraine-hacks-add-worries-cyber-conflict-russiahttps://www.nato.int/cps/en/natohq/news_190850.htm

MISP: NATO's MALWARE INFORMATION SHARING PLATFORM: MODEL FOR UKRAINE?

Upping the ante with what may be another potent bargaining chip, NATO Secretary-General Jens Stoltenberg assured that NATO will continue to provide strong political and practical support to Ukraine in light of these attack, including access to NATO's malware information sharing platform, MISP. See *NATO Secretary-General Stoltenberg Condemns Cyber-Attacks On Ukraine, Promises Enhanced Cyber Cooperation,* January 14, 2022*,* https://ukranews.com/en/news/827060-nato-secretary-general-stoltenberg-condemns-cyber-attacks-on-ukraine-promises-enhanced-cyber

NATO has worked closely with Ukraine for years to help strengthen its cyber-defense capability, and NATO cyber experts in Brussels have been exchanging critical information with their Ukrainian counterparts on the current spate of malign cyberactivities believed to originate in Russia. Indeed, NATO and Ukraine are now on track to sign an agreement on enhanced cyber cooperation that will include providing Ukrainian access to

NATO's MISP, its malware information sharing platform. NATO's strong and practical support for Ukraine will continue.

RUSSIAN NATION-STATE ACTORS

The top three countries targeted by Russian nation-state actors were the United States, Ukraine and the UK. These are just a few of the insights in the second annual Microsoft Digital Defense Report 2021 was released on October 7, 2021. Accessible online at https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/

The report covers the period from July 2020 to June 2021, and its findings cover trends across nation-state activity, cybercrime, supply chain security, hybrid work and disinformation.

CYBERCRIME AND MODEL LAWS FOR UKRAINE?

Cybercrime and Model laws on computer crime and cybercrime

Cybercrime – especially ransomware – remains a serious and growing plague as evidenced in this year's Microsoft Digital Defense Report. But while nation-state actors mostly target victims with useful information, cybercriminals target victims with money. As a result, the targets often have a different profile. Cybercrime attacks on critical infrastructure – such as the ransomware attack on Colonial Pipeline – often steal the headlines. However, the top five industries targeted in the past year based on ransomware engagements by the U.S. Detection and Response Team (DART) are consumer retail (13%), financial services (12%), manufacturing (12%), government (11%) and health care (9%). The United States is by far the most targeted country, receiving more than triple the ransomware

attacks of the next most targeted nation. The U.S. is followed by China, Japan, Germany and the United Arab Emirates.

CYBERCRIME AS A SERVICE

In the past year, the "cybercrime-as-a-service" economy transitioned from a nascent but rapidly growing industry to a mature criminal enterprise. Today, anyone, regardless of technical knowledge, can access a robust online marketplace to purchase the range of services needed to execute attacks for any purpose. The marketplace has three components.

First, as demand has increased, criminals are increasingly focused on specializing in differentiated off-the-shelf infection kits and increasing their use of automation, driving down their costs and growing their scale. Kits can sell for as little as $66.

Second, separate suppliers provide compromised credentials needed to access people's systems and deploy the kits. Credentials have been reported to sell from $1 to $50 each, depending on the perceived value of the target.

Third, cryptocurrency escrow services serve as brokers between buyers and sellers to ensure the kits and credentials perform as offered. Efforts are underway to identify sophisticated kits that not only provide victim data to the criminal who purchased and deployed the kit but also secretly provide the data to the entity that created the kit.

RANSOMWARE AS ONE OF LARGEST CYBERCRIME THREATS

Ransomware continues to be one of the largest cybercrime threats and, in the past year, it has continued to evolve to become more disruptive. Rather than focus on automated attacks that rely on volume and easily paid low

demands to generate profit, human-operated ransomware uses intelligence gleaned from online sources, stealing and studying a victim's financial and insurance documents and investigating compromised networks to select targets and set much higher ransom demands.

THE CYBERCRIME CASCADE EFFECT

•Maria Grazia Porcedda and David S. Wall, *Modelling the Cybercrime Cascade Effect in Data Crime,* IEEE European Symposium on Security and Privacy Workshops, 2021. Porcedda and Wall explain how a cloud-based, data-rich technological environment is fueling data crime with multiple levels and outcomes of victimization. Data theft, or exfiltration, is now central to most modern cybercrimes. Major ransomware attacks now routinely involve data exfiltration prior to encryption, and hacking is the main cause of data loss. An increasing number of reported incidents relating to the illegal acquisition of data has unfortunately led to confirmation of a disturbing trend, a synergy of sorts: illegal acquisition of data via data breaches not only disrupts businesses and organizations, but also facilitates further criminal activity. Porcedda and Wall argue that big volume data crimes are "upstream" crimes which can be later used to hold for ransom, trade or sell on to other offenders for further criminal purposes. These upstream cyber-dependent cybercrimes, solely dependent on internal technologies, subsequently "cascade" crime downstream to enable cyber-enabled offences such as fraud, that use the advantages of the network, and even cyber-assisted cybercrimes which are simply facilitated by digital technology. This is the cybercrime cascade effect that explains the role played by breached data in the changing nature of cybercrime. In short, once

the genie is out of the bottle, it is hard to put it back in: in the world of data, once the cascade begins, it is hard to stop. But while this cascade is hard to track and counter in practice, there are various tipping points at which information and data cascade downwards to facilitate further crime. By catching offender actions at these tipping points, such as at the point at which data is sold on or dumped, then the subsequent downstream "frenzy" of different types of cybercrimes could be prevented or at least mitigated.

CASCADE MODEL'S SIX STAGES

The cascade model starts with completely unrelated individuals with no desire or intention to collude, but who can collaborate through hackers or other forums to inspire or mentor each other to perpetrate a range of harmful cybercrimes. The cascade model is predicated on six fundamental stages in which the social enablers create multiple, overlapping, offending chains.

1. At stage one, a vulnerability is either identified, learned, or created.
2. At stage two, the decision is made about how to run an exploit to take advantage of the vulnerability.
3. In stage three, the offender acts on the outcomes of the exploits and decides how to dispose of the data.
4. Stage four is where offenders trade the data obtained from the exploit for financial or other gain.
5. Stage five is where the initial data is refined and improved in quality, quantity, or both, to use for further offending.
6. Stage six is where scammers, completed unrelated by the initial data crime, or the original hackers or data sellers, exploit the media frenzy and

public confusion cause by the initial data crime, especially following a widely publicized data breach.

TIPPING POINTS

Tipping points can be identified by refining the cascade effect's steps into decision trees which help explain the different offender actions and identify layers of victimization. Once these tipping points are identified, they can show how upstream data-based cyber-dependent cybercrime can result in further cyber-enabled and cyber-assisted cybercrimes. In this way the tipping points shed more light on the cybercrime processes, preventative strategies, the conceptualization of offenses and their interpretation in legal proceedings. Tipping points can occur at each stage of the cascade model, but in different ways and with very different implications. The tipping point may also depend on whether the information found is of value and fed back into the data crime cycle, which may shed light on whether the motivation of the offenders is economic, revenge, or political.

Such interrelationships may help define the different actor groups, but also shape the links between primary, secondary and tertiary victimization, monetization and the demographics of the offender, the presence of an organized crime groups atop other organized parts of the emerging cybercrime ecosystem. Those who contribute to that cybercrime ecosystem may be data-brokers who buy and sell data, darkmarketeers who provide the darkmarket facilities to sell the data, crimeware as service operators who hire out software to facilitate data crimes, bullet proof hosters who host clandestine websites, and crime IT skills brokers who write code.

INCENTIVIZING EARLY INTERVENTION

Porcedda and Wall advocate for further research into ways to incentivize early intervention to stop the cascade effect and perhaps use the cascade effect model as a useful risk management strategy and a way to help law enforcement focus their resources upon key areas, including assisting in the analysis of the overall seriousness of the offense, the motivation behind the offender's decision to reach one or more tipping points, and a more reliable way of identifying aggravating or mitigating circumstances through placing in context an offender's decision to reach or not reach a particular tipping point, thereby providing a useful indicator of the potential impact of intervention programs that might catch potential cybercriminals early on and divert them to a more useful career track and away from prison.

EU CYBERSECURITY POLICY: MODEL FOR UKRAINE?

•Shjika V.Y.,, *Cybersecurity Policy: The European Union Experience for Ukraine,* 2021.

The objective of the EU's cybersecurity policy is to promote cyber resilience, safeguarding communication and data and keeping online society and economy secure.

Shjika identifies the main gaps in the field of cybersecurity in Ukraine as

1. An ineffective regulatory framework and management system.
2. Low readiness to respond to cyberattacks.
3. Low level of involvement of the professional community and lack of a transformational approach.
4. Poor quality audit of cybersecurity.

As an example of the concrete negative financial impact of its overall low cybersecurity ranking within the Central and Eastern Europe region, Shjika reminds us that in 2017, due to the NonPetya virus, Ukraine lost .5% of its GDP, about 14 billion UAH in monetary terms.

CYBERSECURITY REGULATORY FRAMEWORK

Shjika then turns to measures and ways that an effective Cybersecurity Regulatory Framework can be realized in Ukraine. These consist of the following:

1. Transition to international cybersecurity standards.
2. Imposing industry's cybersecurity requirements and industry-specific cyber-crisis regulations.
3. Defining clear criteria for critical infrastructure facilities.
4. Training for organizations and citizens and fostering a culture of cybersecurity in society.
5. Providing a campaign to raise public awareness in the media.
6. Recognition of international certification for officials involved in cybersecurity and auditing.
7. Developing collaboration with researchers and creation of industry-specific cyberattack response centers.
8. Providing cybersecurity audits according to international standards.

•Yashika Nagpal, *An In Depth Analysis of the Rule of Law in Corruption and International Legal Standards on Privacy* (Multidisciplinary International Journal, vol. 7, 2021).

Nagpal provides a robust analysis of various international legal standards on privacy and demonstrates the extent to which cybercrime law provides

guidelines and standards of conduct and behavior, and cybercrime legislation in turn incorporates substantive, procedural and preventative aspects:

1. **The Asia-Pacific Economic Cooperation** (APEC)'s voluntary Privacy Framework developed in 2004 with 21 member nations, leading to the APEC Cross-Border Privacy Rules System in 2011, with system regulations that include self-assessment, compliance evaluation, recognition/acceptance, and dispute resolution and enforcement.
2. **The Council of Europe's** 1998 Draft Guidelines for Individuals' Protection with Regard to Collection and Processing of Personal Data on the Information Highway, accepted in 1999 by the EU as policy guidelines.
3. **European Union (EU) Data Protection Directive 1995**, 95/46/EC, by which non-EU nations must enact privacy legislation with the same level of limitation as EU countries before personal data can be exchanged between the two. Data Protection Directive 1995 was superseded on May 25, 2018, by the GDPR, the **General Data Protection Regulation**, which acknowledges that people have the right to be forgotten, which means that anybody gathering data on people is required to remove that person's records if they ask for them to be erased on their behalf. The European Convention on Human Rights, ECHR, has an impact on the GDPR.
4. **Organization for Economic Cooperation and Development** (OECD) released Optional guidelines on Privacy Protection and Transborder Flows of Personal Data in 1980 to help establish a global standard for privacy law by defining the word "personal data" and establishing the fair information practice principles (FIPPs) that other nations have embraced

in their national privacy regulations. The OECD approved the *Recommendation on Cross-Border Coordination in the Enforcement of Privacy Laws* in 2007, providing a model framework through which member nations will be more likely to enforce privacy rules since it is based on OECD guidelines, including characterizing in the Recommendation the phrase "Privacy Enforcement Authority."

5. **United Nations (UN)'s International Covenant on Civil and Political Rights (ICCPR),** adopted in 1966, protects private information under Article 17, which provides "a person's personal space, family, home, and correspondence shall not be invaded arbitrarily or unlawfully, nor shall anyone be subjected to unlawful attacks on his honour or reputation. The right to be protected by the law is a fundamental human right for everyone." The UN General Assembly's **Resolution 68/167 on Digital Age Privacy Rights** was approved on December 18, 2013. The resolution references the Universal Declaration of Human Rights (UDHR) in stating that privacy is a basic human right that should be upheld. The UN System issued its **Principles on the Protection of Individuals' Personal Data and Privacy** on October 11, 2021.
6. **GRECO, the Group of States Against Corruption, is the Council of Europe's specialist body against corruption,** and is tasked with overseeing strong anti-corruption standards through an active process of mutual evaluation and peer pressure to identify shortcomings in national anti-corruption policies and prompts legislative, institutional, and practical reforms as needed. These include the most significant instruments in the fight against corruption: **The Criminal Law Convention on Corruption** created in 1999 as well as the 2003 Additional

Protocol, **The Civil Law Convention on Corruption** created in 1999, and other important legislative documents such as the **Committee of Ministers' Resolution (97)** which lays out twenty guiding principles for the fight against corruption. The European Court of Human Rights, ECHR, progressively addresses corruption in its caselaw, demonstrating the many connections between corruption, application of the anti-corruption standards and human rights abuses. In light of the ECHR's and GRECO's adherence to these standards, member states of the Council of Europe are required to adhere to all Council of Europe and international norms relating to the prevention of corruption and the promotion of integrity and timely implementation of GRECO's recommendations.

BUDAPEST CONVENTION ON CYBERCRIME: MODEL FOR UKRAINE?

•Slinko, Yepryntsevm Shapar, Sanokoiev, Harkusha, *Modern Indicators of Financial Crimes Detection and Their Prevention in Ukraine*, Dialnet 2021

•*Implementation of the Budapest Convention on Cybercrime*, December 12-13, 2016, Council of Europe. This article sets forth a clear framework for developing ways to combat financial crimes in Ukraine, using a systematic analysis of the main financial crime modern indicators, theoretical sources, practical measures and international experience. These indicators include the use of false documents and other people's accounts, international payment systems, frequent and complex financial transactions of a confusing nature, amounts and counterparties to a transaction that are unusual for a client, and incomplete or missing payment information. The article includes the core finding that the increase in the level of financial

crime is influenced by the presence of off-shore zones, a low level of accountability for the crime, the reluctance of financial institutions to interact with law enforcement agencies in regard to combating such crime. The level of financial crime counteraction can be increased by conducting an external audit and investigation of financial crimes, establishing international cooperation to combat such crimes, blocking suspicious financial transactions, taking preventative measures and combating related crimes.

•*The Budapest Convention on Cybercrime: A Framework for Capacity Building*, GFCE, Council of Europe, July 12, 2016. The Budapest Convention came into being in 2001. The Convention on Cybercrime of the Council of Europe, opened for signature in Budapest in November 2001, remains the most relevant international agreements on cybercrime and electronic evidence.

PRIMARY OBJECTIVES OF BUDAPEST CONVENTION

The Budapest Convention is a criminal justice treaty that provides member states with three primary objectives:

1. The criminalization of a list of attacks against and by means of computers.
2. Procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards. Capacity building in this connection provides an effective way to help societies meet the challenges of cybercrime, and the success of such capacity building depends on political commitment,

reference to common international standards and continuous participation in international peer reviews.
3. International police and judicial cooperation on cybercrime and e-evidence. Current efforts focus on solutions regarding law enforcement access to electronic evidence on cloud servers.

Since its adoption in 2001, the Budapest Convention has brought into focus the common standards that have enabled societies worldwide to be transformed by information and communication technologies (ICT). Through the Budapest Convention, recognition is now given to the need to strengthen security, confidence and trust in ICT and to reinforce the rule of law and protection of human rights in cyberspace.

MANIPULATION OF PERSONAL AND SENSITIVE DATA

•Gundur, Levi, Topalli, Ouellet, Stolyarova, Chang, & Mejia, *Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context*, April 16, 2021. The rate of cybercrime has been steadily increasing over the past decade and continues likely to be underreported.

CERTS: This uptick in cybercrime has led to formation of digital policing units and CERTS (computer emergency response teams) in jurisdictions worldwide, but the downside is that global law enforcement and the private capacity to investigate and police cybercrime competently are insufficient to respond effectively in real time. This problem of lax or non-existent enforcement and regulation is exacerbated by the quickly evolving and vast nature of cybercrimes, particularly those that involve more effort and cross-

border expense and access difficulties than most offline crimes in the pursue mode.

The fast-paced and transnational nature of cybercrimes and cyber offender strategies make it difficult to study and report on rapidly evolving cybercrimes. In those countries where state-sponsored and state-tolerated cyber offending takes place, limited resources and expertise can compound the inadequacy of mutual legal assistance problems, domestic cases can easily be prioritized over international ones. This has led to a near-term strategies to combat cybercrime by focusing largely on prevention, disruption and resilience.

Our collective knowledge about cybercriminal transactions in the international context centers on (1) the modus operandi of cyber offenders engaging business models and (2) how public and private entities respond to their offending within the context of political, jurisdictional and financial limitations within a given geographical location. This is particularly significant in developing countries with less sophisticated systems and infrastructure to combat more technologically savvy offenders who engage in financial offenses that are simpler and entail effective social engineering techniques that can convince hundreds of individuals to part with their money through deception and fraud.

In contrast, more developed countries would likely see more online theft and hacking by more sophisticated offenders using the digital environment to facilitate cybercriminal activity through more powerful, complex financial

platforms that allow them to take advantage of cryptocurrencies, blockchain technology, dark web exchanges, IoT, mobile banking platforms and unsanctioned payments systems. In developed countries this translates to more high-level investigation and intervention systems and agencies focusing their attention on the most sophisticated actors capable or enacting the highest impact offenses involving cryptocurrency-related businesses, while ignoring small-level offending and low-level offenders carrying out credit card fraud, low level fraud and hacking that results in hundreds of dollars of loss. In a nutshell, the level of resources and sophistication of enforcement required by different governments is asymmetric and has a direct impact on the difficulty and effectiveness of cooperation, coordination, prevention and interdiction efforts

•*Cooperating Against Cybercrime: 20 Years on From the Budapest Convention,* Microsoft EU Policy Blog. The Budapest Convention was initially intended to harmonize cybercrime laws and address the limited number of cross-border investigations into and prosecutions of online crime. Drafted in 2001, the Convention provides a good example of how law enforcement agencies can be balanced successfully with human rights, democracy and the rule of law, the three values protected and promoted by the COE. The Convention has also improved coordination and cooperation between law enforcement agencies in like-mined countries among the 65 countries that have ratified it, including the United States which ratified it in 2006. Russia is a member of the Council of Europe, but it has not ratified the treaty which was developed by the Council of Europe. With the introduction of debate and the final round of negotiations on the Second Additional Protocol (SAP), the focus of the Budapest Convention has more

recently shifted to address the challenges of gathering digital evidence from basic subscriber information needed to identify suspects, to collecting online communication content increasingly hosted by global service providers subject to the laws of multiple jurisdictions. We turn to the SAP now.

SECOND ADDITIONAL PROTOCOL (SAP): MODEL FOR UKRAINE?

The SAP will help improve law enforcement efforts by clearing bureaucratic hurdles to cross-border data access requests, by introducing a comprehensive array of instruments that facilitate judicial cooperation in criminal matters, and by upholding procedural rights standards along with data protection and privacy safeguards. The SAP is also an important step to advance the ease of transatlantic data flows and eventual enactment of an agreement on new European e-evidence access rules as part of a transatlantic law enforcement agreement. A lasting solution can be achieved with the adoption of the e-evidence proposal, ratification of the SAP and a robust EU-US law enforcement agreement, leading to data access for law enforcement purposes through modern, principled bilateral and multilateral agreements, all within a framework that member countries respect each other's national sovereignty as well as the fundamental rights and liberties of all citizens.

TWENTY YEARS AFTER THE BUDAPEST CONVENTION

•Jennifer Daskal & Debrae Kennedy-Mayo, *Budapest Convention: What Is It and How Is It Being Updated?* July 2, 2020. As the world's first cybercrime treaty undergoes an update over 20 years after its initial drafting, we should recall the treaty's initial objectives: harmonize national

laws related to cyber-related crime, support the investigation of those crimes, and increase international cooperation in the fight against cybercrime. During this period of time we have witnessed exponential growth in internet usage, AI, cloud computing, and digitalization of almost every kind of interaction. These advances effectively turn almost all crime into cybercrime, making electronic evidence important to almost every crime.

The increasing challenges to law enforcement are likewise enormous, given the global nature of the internet, the range of electronic evidence relevant and critical to investigating and prosecuting crime from basic subscriber information used to identify perpetrators to content of emails that may be stored in a different country from the one where the crime occurred or where it is being investigated. It can no longer be assumed that evidence critical to a cybercriminal investigation will be held within one's own territorial borders, nor can it be assumed that relevant national interests and data location are in the same place.

SAP KEY PROVISIONS

The key provisions of the draft Section Additional Protocol are (1) language of requests, (2) videoconferencing, (3) emergency mutual legal assistance, (4) direct disclosure of subscriber information, and (5) giving effect to foreign orders for the expedited production of data.

Civil society organizations have weighed in on the emergency mutual legal assistance (MLA) provision, cautioning that the emergency procedures

should be carefully designed to protect privacy and ensure that the procedures are not used as a work-around to what is ordinarily a time-consuming standard MLA process.

Civil society organizations have also expressed concerns about the provision for giving effect in a more streamlines manner to orders from another party for expedited production of data, particularly the requirement that supporting information provided to a receiving country be kept secret from the service provider unless the requesting country gives consent for the service provider to access such information.

TRANSPARENCY AND OVERSIGHT

The Cross-Border Data Forum has suggested that these provisions need to come with transparency, oversight and further protection against abuse, and that sufficient safeguards should be included to mitigate against a law enforcement free-for-all under which any government actor anywhere can simply compel production of data anywhere under domestic authority alone.

INTERNET OF THE FUTURE

The internet of the future will be shape by the success or failure of the proposed amendments to the Budapest Convention reflected in the draft SAP. Those proposed amendments envision a world in which data continues to flow across borders and seeks to adjust jurisdictional rules and limits.

RUSSIA-LED INITIATIVE FOR ALTERNATIVE CYBERCRIME TREATY

Against this effort is another initiative led by China and Russia at the United Nations to create an alternative cybercrime treaty, which these sponsoring countries frame as a means of asserting control over the internet and the data needed for basis governmental functions, including law enforcement. This alternative cybercrime treaty is based on a world view that provides for control to be exercised over the technology to meet pre-established jurisdictional limits, and it is a serious attempt by Russia and China to set the United Nation's rules on cybercrime. In contrast, the Budapest Convention is the only global treaty that exists with a common vision for trying to facilitate international cooperation on cybercrime that also aims to protect the rule of law and an open internet.

DANGERS OF RUSSIA-SPONSORED CYBERCRIME TREATY

•Deborah Brown, *Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights,* Human Rights Watch, August 13, 2021. Human Rights Watch has provided a detailed account of the Russia-proposed global comprehensive treaty to combat cybercrime on which negotiations will start this year. It points to the irony of a Russian government that faces criticism for turning a blind eye to cybercriminals operating within its borders in the emergence and sudden disappearance of REvil, a cybercrime group behind a massive ransomware attack that swept through businesses worldwide in early July 2021. Human Rights Watch warns that this Russian proposal is dangerous and can lead to a binding international treaty with the potential to expand government regulation on online content and reshape law

enforcement access to data in a way that could criminalize free expression and undermine privacy.

It does matter who is proposing the treaty, the way many states have defined "crime" in the cyber context, how efforts to fight cybercrime have undermined rights and the shortcomings of multilateral negotiating processes that reveal the danger posed by this treaty process. Along with the surge in cybercrime laws worldwide, some of those laws have been overly broad and have undermined human rights.

Governments often use such laws to persecute journalists, human rights defenders, technologists, opposition politicians, lawyers, religious reformers and artists. Many governments, including those most supportive of a global treaty on cybercrime, treat forms of free expression such as criticism and dissent as crimes. A cybercrime treaty that normalizes this approach runs counter to human rights obligations.

"CYBERCRIME" FEARS AS COVER TO CRACK DOWN ON RIGHTS

Many of the governments leading the Russia- and China- sponsored global comprehensive cybercrime treaty use cybercrime as a cover to crack down on rights. In what is already a heightened atmosphere of political polarization, opposition to this treaty is made of up the United Nations, the US, the EU, and many states that are already parties to the Budapest Convention. The opposition has come from 93 states either voting against or abstaining from the 2019 resolution to set in motion the process to draft the global treaty, compared with 79 votes in favor of it. Key questions still remain about what

constitutes cybercrime, how far law enforcement should gain access to data for cross-border investigations, and the role of governments in regulating the internet, all questions with serious implications for human rights, freedom of expression, association, privacy and due process.

EFF: PRIVACY SAFEGUARDS LACKING

The Electronic Frontier Foundation, an international digital rights group, has criticized the Second Additional Protocol to the Budapest Convention for lacking strong privacy safeguards and placing few limits on law enforcement data collection. EFF takes the position that the SAP can endanger technology users, journalists, activists, and vulnerable populations in countries with flimsy privacy protections and can weaken everyone's right to privacy and free expression across the globe. Civil Society Organizations have customarily been invited by Council of Europe committee sessions to participate in drafting plenary meetings, but this was not the case in the negotiations over the SAP, despite the fact that over 100 organizations called for transparency in the process. As a consequence, multilateral negotiations in this process have excluded civil society organizations and others who are rights defenders, especially on issues like cybercrime that are considered the domain of law enforcement.

II. PRIVACY AND DATA PROTECTION

Data theft and manipulation by state and non-state actors;

•Jay F. Kramer & Sean B. Hoar, Lewis Brisbois, *GDPR, Part 1: History of European Data Protection Law,* 2016. This is a helpful analysis of how the GDPR will affect commerce among and between three of the world's most

significant markets: the United States, the European Union and China. It traces today's GDPR back to the EU's 1995 Data Protection Directive 95/46/EC, and to its predecessor, the OECD's 1980 issuance of international data privacy and protection guidelines known as *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, which established key principles of data protection and privacy reflected in today's GDPR. Key principles established by the OECD in 1980 were in a non-binding and voluntary framework, and a mosaic of European privacy laws resulted from that framework, which ultimately became the global standard for fair information practices. They included (1) the purpose of data collection should be relevant to its use, (2) data should be protected against loss and unauthorized access, (3) individuals should have the right to know what data is collected about them, (4) individuals should have the right to access any data related to them, and (5) an individual should be able to challenge the retention of data, or amend or erase data about him or her.

ADEQUATE LEVEL OF PROTECTION

When the European Commission (EC) promulgated a new Data Protection Directive 95/46/EC, each member state was required to adopt privacy laws that were the equivalent of one another. It also directed that data could only be exported to third party countries that could ensure an "adequate level of protection" for European citizens' data through their domestic laws or through international commitments that had been made.

SAFE HARBOR FRAMEWORK

The EC approved a "safe harbor" framework in July 2000 that had been developed by the U.S. Department of Commerce to establish a set of fair data information practices to which participating organizations agreed to abide. Those organizations participating in the framework also agreed to enhanced enforcement and oversight by the U.S. Federal Trade Commission (FTC) and the U.S. Department of Transportation (DOT).

•Dr. Abdulah M. Aseri, *The Implications of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy*, Journal of Theoretical and Applied Information Technology, vol. 98, No. 4, February 29, 2020. Data privacy is important to both consumers and organizations, and fundamental rights and freedoms can be damaged by a breach of personal information. Data privacy is thus a critical aspect of the GDPR implementation and adoption for global firms and organizations.

The GDPR through a regulated approach in the data handling procedures has a business influence of necessitating a proactive approach in the management of consumer data. GDPR requires multinational firms to limit data transfers across different platforms while ensuring they undertake to critically design information systems as a priority in enhancing consumer protection. In this context, GDPR has a cumulative effect of enforcing multinational business compliance with local state laws and EU consumer data and security protections.

THE DIGITAL "WILD WEST": MODEL FOR UKRAINE NEEDED

•Kobrin, Korchynskyi & Nekrutenko, *Ukrainian GDPR: The Reality and Future of Privacy Legislation in Ukraine,* International Association of Privacy Professionals, September 28, 2020. The state of regulation of personal data processing in Ukraine has been described as a digital "Wild West", a factor that likely contributed to the EU's decision in 2017 to fund a Twinning Ombudsman project with a budget of €1.5 million to help Ukraine bring its data protection system in line with international and European standards. The initiative completed its work in November 2018, with over a dozen recommendations and methodologies for the effective implementation of the data protection reforms.

The draft legislative act was never brought to the Ukrainian Parliament, nor was the implementation stage covered publicly. The results of this project's work remain unused. Privacy HUB, a Ukraine-based NGO has prepared this report on Ukrainian GDPR to explain the current state of personal data protection in Ukraine, what can be done to change the paradigm, and how to succeed in striking a balance between the public and private interest in reform initiatives.

Current enforcement of privacy in Ukraine lacks resources and independence, and there is a growing need to establish an independent and non-subordinate regulatory body that goes beyond the data protection supervision and control in Ukraine carried out by the Verkhovna Rada's Commissioner for Human Rights, which is a Parliamentary ombudsman

overseeing human rights protection in general and not a stand-alone data protection authority.

MINISTRY OF DIGITAL TRANSFORMATION: DIAA ONLINE PORTAL

Ukraine's digitalization strategy is centered in the Ministry of Digital Transformation, and the protection of personal data is a priority of the ministry, forming the culture on how to address the issue of personal data approaching EU standards. The ministry's projects, including national portal Diia, an online platform for digital literacy Diia and the Diia.Business application, are reviewed and approved by the internal group on data protection. Ukraine's Ministry of Digital Transformation has launched the Diia online public services portal, Deputy Prime Minister, Minister of Digital Transformation Mykhailo Fedorov has reported on his Telegram channel, stating that "We have launched the Diia portal that will become a universal point of access for Ukrainians to all electronic services." According to Fedorov, services for sole proprietors are the first services available on the portal. "For more than a month, testers opened a sole proprietor enterprise, closed it, and made changes to it. Now every Ukrainian who has dreamed of starting a business will be able to do it without queues." Starting a business in Ukraine is now the fastest and most convenient process among similar services in the world, and Federov explains that in order to access the services, it is necessary to log in in the citizen's cabinet, which includes data from registers about business, real estate, vehicles, land plots and digital documents from the Diia application.

In total, Ukrainian citizens can now get 27 public services online on the Diia portal. Each group consists of various professionals with different backgrounds that complement data protection.

STRONGER PRIVACY CULTURE & DATA PROTECTION POLICY

This Ministry of Digital Transformation also proactively promotes privacy and personal data protection to prevent privacy incidents and data breaches, and provides assistance in the improvement of public registers, deletion of duplicated or inaccurate data, controls any changes, or access to the registers. Internal procedures have been implemented by the Ministry of Digital Transformation on how to process personal data of its workers, with privacy notices in place for the users of its application and websites, as well as a data breach and incidents policy and procedures review and adoption of projects, and a specific procedure that prohibits launching new projects without a preliminary data protection audit. Data protection training and education are a common practice for those serving in the ministry. The ministry is a driving power for strengthening privacy culture and regulatory policy in Ukraine and will be a substantial factor leading to broader promotion of data protection in Ukraine.

- Linden, Khandelwal, Harkous, and Fewaz*, The Privacy Policy Landscape After the GDPR,* Sciendo, Proceedings on Privacy Enhancing Technologies, January 7, 2020. As one of the most demanding and comprehensive privacy regulations to date, the EU GDPR overlies a landscape of privacy policies that are in transitional phases in some states, with many policies still not meeting several key GDPR requirements or are attempting to cover more practices at the expense of specificity.

•*Code of Practice on Disinformation,* 2021: The Code of Practice addresses the spread of disinformation, and is the first time worldwide that industry has agreed voluntarily to self-regulatory standards to fight disinformation. It set a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation. The Code was signed by Facebook, Google and Twitter, Microsoft, TikTok, Mozilla and other online platforms and players from the advertising industry.

THE EU DIGITAL SERVICES ACT: MODEL FOR UKRAINE?

Sandor Zsiros, *What is the EU Digital Services Act and how will it impact Big Tech? EuroNews* 1-20-2022

In December 2020 the European Commission published a final proposal for a new legislative framework, the Digital Services Act (DSA), to tackle challenges like the sale of fake products, spreading of hate speech, cyber threats, limiting of competition, and market dominance. The DSA once enacted will modernize the e-commerce directive of the EU, its underlying premise being that what is illegal in the real world should be illegal in the online world as well. The DSA will affect platforms and online intermediaries used by hundreds of millions of Europeans every day and will include social media platforms like Facebook and Twitter, app stores, video and music sharing platforms like YouTube and Spotify, Airbnb and similar online travel sites, and other digital marketplaces. Users will be able to flag illegal content, with the platform then obligated to notify them of any decisions. A system of trusted flaggers will be established for entities with special expertise in a particular area. In short, the DSA aims to create a

safer online world, enabling users to have a say on what they see online, regulating targeted advertising and targeting online hate speech, disinformation, and counterfeit products, with sanctions imposed on platforms if they fail to act.

As the EU moves closer to finalizing the Digital Services Act, it will be a milestone in how internet giants are regulated and will provide tightened security for users. In late January 2022, the European Parliament overwhelmingly approved its position for negotiations with member states and the European Commission, as they seek to hammer out the fine details before it eventually becomes law. The European Parliament will need to conclude talks with both the EU Council and the Commission, after which the European Parliament will need to vote on and approve the final version of the legislation, which will have to be applied in member states before becoming effective as law.

•*Revision of the Code of Practice: The strengthened Code Expected by March 2022,* December 2, 2021. The strengthened Code of Practice is expected to evolve towards a co-regulatory instrument by March 2022, as outlined in the EU Digital Services Act, *supra*. Joining the Code of Practice means becoming a part of an EU-wide, innovative and robust framework that aims to provide users with appropriate safeguards with regard to the misuse of online services to spread disinformation.

•Benjamin E. Griffith & Sven Kohlmeier*, The Right of Privacy under American and German law: A Comparison of Perspectives, International Municipal Lawyers Association Berlin Conference,* November 3-8, 2019.

Benjamin E. Griffith & Sven Kohlmeier provided a current discussion on the right of privacy from the perspective of American lawyer and a German Rechtsanwalt. They addressed differences and similarities between the U.S. privacy laws, the CLOUD Act of 2018, data privacy and privacy protections as well as laws that reflect Germany's approach to the right of privacy, data protection and security, the Network Enforcement Act (NetzDG), the German Federal Data Protection Act, and the European Privacy Standard of 2014 that gave rise to the Right to be Forgotten. Their presentation was given in Berlin and moderated by the Berlin Data Protection Office, touching on implementation of and extraterritorial protection provided under the GDPR, facial recognition technology, computational propaganda and online privacy challenges faced by Google, Facebook and other social media giants. The differences are global in nature, transnational in scope and rooted deeply in history. The similarities center on possible collaboration between the U.S. and the E.U. and reflect the closeness of these two nations in the field of human rights, governmental oversight, individual freedom and the fundamental right of privacy.

DISRUPTION AND WEAPONS OF MASS DISTRACTION

•Christina Nemr & William Gangware*, Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age,* March 2019. If there is one word that has come to define the technology giants and their impact on the world, it is "disruption." Beyond the traditional sectors that have been upended by major tech and social media companies, disruptive attacks have been aimed at one another, with more insidious trade-disinformation and propaganda, often with messages conveyed through

disinformation ranging from biased half-truths to conspiracy theories to outright lies. Uncertainty, fear and anger are the very characteristics that increase the likelihood of a message going viral. Networks consisting of fake profiles amplify the message and create the illusion of high activity and popularity across multiple platforms at once gaming recommendations and rating algorithms. These techniques for spreading fake news are effective: a fake news story reaches 1500 people six times more quickly that a factual story, with false stories about politics being most likely to go viral. Disinformation resonates, and it is difficult to debunk. State-sponsored media manipulators know this very well.

Now let's take a closer look, drawing the following discussion and analysis from Christina Nemr and William Gangware's *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age,* accessible online at Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf. At present, Russia's information warfare machine functions like a diverse and interconnected ecosystem of actors, including state-backed media outlets, social media accounts, intelligence agencies and cyber criminals. Although many of the hallmarks of Soviet propaganda are present in Russia's modern-day propaganda efforts, what had changed it the speed with which the narratives are created and disseminated.

Before 2016, Russia honed its online disinformation efforts in its immediate sphere of influence. Russia deployed a coordinated online influence campaign during its annexation of Crimea in 2014. Russian state-controlled

media outlets painted a uniquely anti-Ukrainian, pro-Russian narrative surrounding then-President Viktor Yanukovych's flight from Ukraine and the subsequent Russian invasion of Crimea.

To help shore up domestic support for Russia's actions, Russian government bots dominated the domestic political conversation in Russia during this period. Between 2014-2015, as much as 85 percent of the active Twitter accounts in Russia tweeting about politics were, in fact, government bots. In mid-2016, the Kremlin unleashed these tactics during the United Kingdom's successful June 2016 referendum vote to leave the European Union. One analysis of tweets found that in the 48 hours leading up to the vote, over 150,000 Russian accounts tweeted about #Brexit and posted more than 45,000 messages about the vote. On the day of the referendum, Russian accounts tweeted 1,102 times with the hashtag #ReasonsToLeaveEU. Meanwhile, Russia was deploying a similar strategy during the 2016 US presidential campaign, with its secretive Internet Research Agency headquartered in a heavily-guarded building in downtown St. Petersburg. On one floor, employees produced a high volume of fake articles, using mostly original text to create a veneer of authenticity, and on another floor a separate group of employees created fake social media accounts to distribute these articles and then post comments about them.

An NBC report identified 2,752 Russian "troll" accounts that posted more than 200,000 tweets; these tweets earned 2.1 million retweets and 1.9 million likes. Twitter reported an even more expansive campaign that likely extended beyond the IRA, with 36,000 automated accounts posting 1.4

million tweets that earned 288 million views leading up to the election. On Facebook, Russian posts reached 126 million US Facebook accounts. On Instagram, which is wholly owned by Facebook, 170 Russian accounts created more than 120,000 pieces of content, which reached more than 20 million US accounts. The activities of the IRA were not limited to Facebook, Instagram, and Twitter; it also targeted YouTube, Google+, Vine, Meetup, Pinterest, Tumblr, Gab, Medium, Reddit, and even PayPal, which helped sell its merchandise. The IRA's activities on Instagram were particularly effective at generating impressions. Instagram's platform is conducive for posting the most viral content – jokes and memes – and Russian accounts leveraged this platform to maximize their reach. Between 2014 and 2017, IRA content on Instagram reached 187 million engagements (likes and shares), far exceeding their content's 76.5 million engagements on Facebook.

The New Knowledge Report on the Internet Research Agency's disinformation tactics predicted that "Instagram is likely to be a key battleground on an ongoing basis." It is clear that there was a significant volume of Russian posts and impressions generated during the 2016 US presidential campaign. However, some have cautioned against exaggerating the impact of Russian disinformation on the outcome of the election.

As noted in *Weapons of Mass Distraction*, most Americans probably only scrolled past a very small number of Russian-backed posts throughout the duration of the 2016 campaign, which says nothing about whether they read, clicked on, or were influenced in any meaningful way by the content. Furthermore, the several hundred million impressions of Russian

propaganda across Twitter and Facebook during the campaign were dwarfed by the billions of total daily impressions of all content across both platforms. Kremlin-generated impressions were a drop in the bucket compared to total user activity, which calls into question their ability to have played a decisive role in swaying public opinion. Russia's ad-targeting also appeared to lack an overarching electoral strategy: less than $2,000 was spent on Russian ads in the battleground state of Wisconsin, and even less on the battleground states of Pennsylvania and Michigan, suggesting that Russian content did not deliver meaningful impact on the electoral college votes that decided the election.

Others have argued that the IRA's disinformation campaign was amateurish and careless, even failing to hide the origin of its content, which further underscores the need for caution when assessing the effectiveness of its propaganda. It is perhaps more plausible that Russian cyberhacks into the Clinton campaign - rather than the Kremlin's social media disinformation - impacted the course of the election. Kathleen Jamieson, the director of the Annenberg Public Policy Center at the University of Pennsylvania, has argued that the disclosures from WikiLeaks' release of Russian-hacked Clinton campaign emails caused the decline in polled voters' trust in Clinton in October 2016. In the wake of the 2016 election, the Kremlin appeared intent on continuing to leverage disinformation to influence political discourse in the United States and elsewhere. Indeed, US sanctions and condemnations seem to have done little to dissuade the Russians from maintaining these efforts. While the IRA spent $12 million during the 2016 election campaign, its budget totaled $12.2 million in 2017

and $10 million for the first half of 2018 leading up the US midterms. Russian posters have also adapted their tactics, shifting away from producing fictional content which can be censored by platform moderators, towards amplifying existing political memes promoted by far-right and far-left sources.

Addressing the question of who should bear responsibility for countering disinformation, the simple-appearing answer may be appealing. When states like Russia or Iran spread disinformation on Facebook or Twitter, they are not doing so to attack Facebook or Twitter. They are doing it to undermine geopolitical adversaries, including the United States. Governments, then, seem to bear the ultimate responsibility for defending their nations against this kind of disinformation. However, that answer obscures a major complication: the battleground rests firmly in private hands.

GOVERNMENTAL REGULATION OF SOCIAL MEDIA COMPANIES

There may be a greater role for governments to play in engaging with and regulating social media companies. After all, online platforms, while well-resourced both financially and technically to wage this battle, do not necessarily have perfectly-aligned incentives with governments who are seeking to guard against foreign meddling. Nor are they necessarily capable of defending against every effort from sophisticated hostile actors. On the other hand, significant government involvement carries its own risks, including the potential for impinging upon freedom of expression and outright censorship. However, certain tailored regulations may avoid such

limitations. For example, Guillaume Chaslot, a former YouTube software engineer, has suggested holding technology companies legally liable for their algorithmic recommendations, as opposed to every piece of content they host. Such an approach could protect freedom of expression while still holding social media companies accountable, and incentivized, to prevent their platforms from recommending disinformation-related content. In the absence of clear delineations of responsibility, a reasonable next step could involve greater collaboration between technology companies and governments. A productive public-private relationship would enable transparent information sharing, fact-finding, and the development and deployment of targeted solutions meant to quickly counter foreign disinformation online.

Other potential models for countering foreign disinformation online come from the world of financial crimes enforcement, where several frameworks promote cooperation between governments and the financial sector to better identify and disrupt money laundering and terrorist financing.

FINANCIAL ACTION TASK FORCE: MODEL FOR UKRAINE?

One prominent example is the inter-governmental Financial Action Task Force (FATF), which encourages information sharing between financial institutions, law enforcement authorities, and governments. The FATF works to identify country-level vulnerabilities, promote regulatory reform, and leverage new technologies to confront money laundering and terrorist financing across its 37 member states. Given the numerous actors that shape and are shaped by the information and digital landscape, addressing

disinformation will require ongoing and open cooperation. There is no single solution or silver bullet to address this complex problem. However, social media and technology companies are well-placed to lead these efforts, in collaboration with governments and other partners.

Three key challenges facing these efforts to counter disinformation were identified in Weapons of Mass Distraction.

1. First are technology gaps. Many observers classify the modern disinformation environment as an arms race in which researchers, technologists, and governments scramble to develop tools to detect, counter, and keep pace with nefarious actors' methods and activities. This environment is characterized by a wide availability of sophisticated technologies that, until recently, were concentrated in leading tech companies or research labs.
2. The second set of challenges is structural. These relate to the economic incentives of developing counter-disinformation technology, the dearth of available data sets to train machine-learning tools, and the slow rate of adoption of existing tools.
3. The third and final category of challenges relate to the gap in understanding exactly how technologies – such as AI – are evolving, and with it, the threat from disinformation.

PUBLIC -PRIVATE PARTNERSHIP MODEL

What emerges from this excellent but incomplete discussion of how to stop disinformation is a proposal for a public-private partnership model, a possible approach for harnessing diverse expertise to solve the disinformation problem. Aligning industry and technical experts with the

lawmakers who shape public policy will help produce an informed and measured response to a complex, rapidly transforming threat. It is to be expected that competing interests and incentives will hinder coordination, but a collaborative public-private framework is a prudent foundation on which to build consensus and coordinate action

Principles of personal data processing (legality, fairness, transparency, purpose limitation, data minimization, accuracy, data protection, integrity, and confidentiality):

•Melnyk, Kostenko, Blinova & Shynkarenko, *Experiencing Personal Data Protection on the Internet and Its Possibilities of Recognition and Enforcement in Ukraine,* Revista de Derecho, vol. 10 (II), April 12, 2021. This article evaluates the most successful ways, forms and methods of personal data protection on the internet among foreign countries for domestic and legal purposes. One of the key tasks facing modern jurists and judicial officers is the protection and proper confidentiality if personal data of individuals, which is very closely related to the institution of intellectual property. The level of protection of personal data of individuals in a country is a key indicator of the extent to which a state meets the criteria of freedom, democracy and the rule of law.

Turning to Ukraine, internet penetration in Ukraine has annually increased by an average of 5%, with 49% internet penetration of households in 2015, 63% in 2016, 70% in 2018, and 73% in 2019. Any effective legislation that is formulated and proposed for enactment on the subject of personal data protection must be based on such well-known international documents and standards as the Universal Declaration of Human Rights of 1948 (UDHR),

and the International Covenant on Civil and Political Rights of 1966 (ICCPR), both ratified by the Verkhovna Rada, the Ukrainian Government. Current legislation of Ukraine on personal data protection consists of the Constitution of Ukraine, the Law of Ukraine on Personal Data Protection, and other laws and international treaties of Ukraine that were approved as binding by the Verhovna Rada. Member states of the European Economic Area and states that have signed the Council of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* are also recognized as ensuring an adequate level of protection of personal data. Melnyk et al conclude that the legal protection of personal data on the internet should be carried out with the help of special simplified procedures for amending and adopting new legal legislative acts. The best role models for Ukraine in the field of proper protection and ensuring the confidentiality of personal data on the internet are the United States and the European Union member states, since these countries have common values regarding the priority of human rights, freedoms and interests of the individual over the State, as well as developed means of successfully protecting these values.

- *European Union General Data Protection Regulation (GDPR) and United States of America Clarifying Overseas Use of Data (CLOUD Act: David versus Goliath),* 2018. The history of data protection laws in Europe and North America are interlinked with the fundamental rights to privacy, and the story of data protection is essentially the story of the right of privacy within Constitutional Law. The UN Universal Declaration of Human Rights forms the underpinning for modern international Constitutional Law interpretations of privacy as an integral ingredient of human dignity.

Protection of privacy as an inviolable right to one's family and all communications therein is enshrined in most of the Constitutions within the modern states. The UN Charter further extends to data protection in the more modern versions of Constitutional Law where it specifies protections for personal data. The EU recognizes data protection as a distinct right in Article 8 of the Charter of Fundamental Rights.

THE CLARIFYING OVERSEAS USE OF DATA ACT

The US CLOUD Act of 2018 was a back-door piece of legislation that was snuck into the 2,323 pages of a $1.3 Trillion federal government spending bill, the Consolidated Appropriations Act, 2018 PL 115-141. The 2,323 page legislation, with the CLOUD Act attached, was handed over to the U.S. House of Representatives after 8:00 pm on Wednesday, March 21 for review and approval for a floor vote the next morning, Thursday, March 22, 2018. By a vote of 256 to 167, the U.S. House of Representatives approved the federal government spending bill, with the CLOUD Act attached. That same night, on March 22, 2018, the U.S. Senate approved the legislation with a 65 to 32 vote and send it to President Donald Trump for his signature, and he signed it on Friday, March 23, 2018. In this way and under these time constraints a globally significant law was enacted in the form of the CLOUD Act of 2018, HR 4943 and S 2383. The *Clarifying Overseas Use of Data Act* was the culmination of a long series of legal battles on both sides of the political aisle (and both sides of the pond) to tackle the uncertainties that occurred with the lawful handling of Big Data, and provide a complex legal structure that will affect the future handling of personal data for those using internet technologies.

The CLOUD Act of 2018 provided a means to access data held abroad by US-based companies, but also created incentives for other jurisdictions to enter into executive agreements with the United States over data transfer. A similar regulatory measure in the form of the EU's E-Evidence Regulation is now under consideration in the European Union, and could provide the foundation for a possible EU-US framework agreement which would facilitate the reciprocal transfer of criminal data between the EU and the US.

•Stephen P. Mulligan, *Cross-Border Data Sharing under the CLOUD Act*, Congressional Research Service, 7-5700, April 23, 2018. The CLOUD Act was enacted as one of the first major changes in years to U.S. law governing cross-border access to electronic communications held by private companies. Its first component addresses the U.S. Government's ability to compel technology companies to disclose the contents of electronic communications shared on the companies' servers and data centers overseas. The second component addresses the reciprocal issue of foreign governments' ability to access data in the United States as part of their investigation and prosecution of crimes. The CLOUD Act modernized the process by which the executive branch can conclude a new form of international agreement under which select foreign governments can seek data directly from U.S. technology companies without individualized review by the U.S. Government. It accelerates the process by which law enforcement officials in the U.S. and abroad can seek access to electronic communications such as emails and social media posts that are stored on servers and in data centers located in foreign countries. The CLOUD Act will likely provide a clearer definition of the scope of U.S. officials' right to seek certain data stored

overseas in the custody of U.S. providers, but it will also have a much broader and much less certain impact on the international data sharing regime. Law enforcement officials worldwide can be expected to continue to seek access to data stored on servers outside their territorial jurisdiction. This level of data access will have an impact on privacy, human rights, and civil liberties interests, but unfortunately it will come with an uncertain degree of potential for abuse of the system and potential for inadequate protections for privacy, human rights and civil liberties.

•Karpenko, Kuczabski & Havryliak, *Mechanisms for Providing Cybersecurity During Covid-19 Pandemic: Perspectives for Ukraine* (Security & Defense Quarterly, vol. 33, January 2021). In the context of cybersecurity in the medical sphere, there has been a shift of emphasis from the problem of protection of personal data of patients to the protection of key functions of the medical sphere. There are mechanisms to implement cybersecurity to counter the spread of fake news, disinformation and misinformation on the internet that have surfaced during the COVID-19 pandemic. Those practical tools and cybersecurity measures used during the pandemic are recommended for Ukrainian authorities, and they will provide a way to ensure a balance between the implementation of restrictive policies in the field of cybersecurity and ensure freedom of speech and openness of the internet.

UKRAINIAN EXPERIENCE IN SECURITY ISSUES DURING PANDEMIC

To curb the spread of COVID-19 in Ukraine, a mobile app "Act at Home" was launched. Its basis is the experience of countries that use digital tools to ensure the safety of citizens during a pandemic. Prior to the pandemic,

Ukraine already had significant e-government experience. In particular, the population was largely ready to use virtual forms of interaction with government agencies. However, some problematic issues remained:

- the traditionally low level of law-abiding citizens, which created problems with frequent evasion of the "Act at Home" application;
- the significant legal ignorance of the population about the requirements of the system and the possible consequences of evading its application;
- insufficient administrative and managerial discipline, which caused some chaos in terms of its practical application;
- deficient organizational culture, which arose in the effective cooperation of various services in the project: border authorities, health care facilities, police, social services;
- corruption and lobbying of individual medical laboratories that made money from clients who wanted to avoid long-term quarantine.

THE ACT AT HOME APP

The "Act at Home" app's functions are as follows:

- Confirmation of the location of self-isolation with location determination;
- Photo confirmation of stay at the place of self-isolation;
- Emergency call to the Ministry of Health of Ukraine hotline;
- Planned functions for monitoring symptom development.

The "Act at Home" app is designed to maintain contact with the person and control the observance of obligatory self-isolation during the quarantine. It

provides benefits during self-isolation, but installation is voluntary. It can only be installed by citizens with Ukrainian phone numbers.

The "Act at Home" app allows the user to confirm the location of self-isolation with the definition of geolocation, provide photo confirmation of the location of self-isolation, make an emergency call to the hotline of the Ministry of Health of Ukraine and monitor the development of symptoms. The app should be installed by people who came from countries in the "red zone" and must undergo a 14-day quarantine. An alternative to self-isolation is to take a PCR test in one of the Ukrainian certified laboratories. According to the Ukrainian legislation, every citizen of Ukraine who has returned from the "red zone" does not want to undergo self-isolation for 14 days and wants to pass the PCR test to cancel self-isolation, must act according to the described algorithm:

- Install the "Act at Home" app, indicating the user's phone number and place of self-isolation;
- After crossing the border, reaching the place of self-isolation within 24 hours;
- During this time, the application will automatically remind the user to mark whether a person has arrived at the selected location;
- Within 24 hours, it is possible to take a PCR test in a certified laboratory/clinic.

During the PCR test, the person must tell the laboratory/clinic representatives the phone number linked to the "Act at Home" app and fill in the consent for data processing. The agreement should establish that the border of Ukraine has been crossed and if this occurred in the last 14 days

and the exact date of arrival in Ukraine. After passing the PCR test, the person should go to the place of self-isolation and indicate that they have arrived in the “Act at Home” app. The PCR test result should be ready within 24-48 hours. Employees of the certified laboratory/clinic independently transmit information about a negative PCR test result to the electronic system of the Public Health Centre of the Ministry of Health of Ukraine, indicating the person’s phone number linked to the “Act at Home” app.

Abiding by self-isolation rules with the use of the “Act at Home” app is monitored with the help of regular messages at optional intervals throughout the day and verification of the person’s face photo with the reference photo taken at the time the mobile app was installed, as well as the geolocation of the mobile phone at the time of photographing. If the user receives a message, the user needs to take a photo of his or her face against the background of the environment within 15 minutes, so always keep one’s smartphone close by. Messages won’t be sent at night.

If a person chooses self-isolation with the “Act at Home” app, this person must confirm this decision when passing passport control – first by providing a personal phone number and the address of the self-isolation place, and then showing the appropriate app screen to the State Border Service employee.

To get started with the “Act at Home” app, the person needs to enter the mobile phone number of the Ukrainian mobile operator, which will be active for the next 14 days. The number should receive a short SMS message with the code that must be entered for registration and, after permission to send messages is granted, the person should fill in information about the place of

isolation (residence). After filling in the data about the place of self-isolation, the application will show a window “Are you already at the address of self-isolation or observation?”. Upon arrival at the place of isolation, it is necessary to confirm arrival at the address of self-isolation and send a reference photo, which is also the recorded geolocation. In the future, artificial intelligence will compare the following photos, which should coincide with the reference photo. From the moment of authorization, the person is considered to have chosen to exercise control with the help of the “Act at Home” app and can undergo self-isolation at the place of residence. After the user takes his reference photo, the main screen will open in the application with a counter of days until the end of quarantine. The countdown starts from 14 days. On the last day of self-isolation, the counter will show «0 days of self-isolation or observation left». When the self-isolation period expires, the message “Your self-isolation or observation period has expired” will appear instead of the counter, and the “Log out” button will become active, with which the user can log out of the application and delete if desired.

The experience of using the “Act at Home” platform in Ukraine has revealed several problems related to security issues, in particular concerning the impact of the poverty factor, which has reduced the effectiveness of the mechanism copied from the practice of rich countries. Nagy (2019) claimed that Ukraine is at a very early stage of the evolution into a multiscreen nation. He noticed that although the number of Internet users in Ukraine is growing rapidly and steadily, it is still significantly lower (66%) than it was in Hungary five years ago.

The grounds for processing personal data by the "Act at home" app are defined in the Law of Ukraine No. 555-IX dated Apr. 13, 2020, *On Amendments to the Law of Ukraine On Protection of Infectious Diseases to Prevent the Spread of Coronavirus Disease (COVID-19),* according to which for the period of quarantine or restrictive measures related to the spread of coronavirus disease (COVID-19), and within 30 days of the date of its cancellation, the processing of personal data is allowed without the consent of the person, including data relating to health, place of hospitalization or self-isolation, surname, name, patronymic, date of birth, place of residence, and work (study), in order to counteract the spread of coronavirus disease (COVID-19), in the manner specified in the decision to establish quarantine, provided that such data is used solely for the purpose of anti-epidemic measures» (The Law of Ukraine, 2020).

At the same time, experts (Deutsche Welle, 2020a) are concerned about the technologies used in such coronavirus tracking apps, which enable governments to collect personal information. It also can lead to mass state surveillance, as well as the violation of the traditional balance of rights and freedoms of citizens in the digital space.

Coronavirus tracking apps may pose such personal security risks as:

- Deanonymisation of people who are in self-isolation or under observation;
- Unreasonable control over specific people through tracking their geolocation and movement;
- Using of personal data outside the official purpose for which it is legitimately collected;

- Processing information about individuals outside the time limits established by national legislation;
- Unauthorised interference with the operation of mobile devices in which mobile apps are installed.

MISINFORMATION ABOUT COVID-19 AS A GLOBAL THREAT

One of the current challenges today is the outbreak of disinformation about COVID-19. Although COVID-19 is not the first pandemic in history, it is the first to be covered so massively and with lightning speed. And the «fault» for this, oddly enough, lies with the internet and the technical privileges of this century.

Since the beginning of the coronavirus pandemic, the World Health Organisation has emphasised that not only COVID-19 but also false information about it poses a threat. False or misleading information about the coronavirus is primarily a threat to public health. The 2019-nCoV outbreak and response has been accompanied by a massive «infodemic» – an over-abundance of information – some accurate and some not – that makes it hard for people to find trustworthy sources and reliable guidance when they need it (World Health Organisation, 2020).

UKRAINE'S IMPLEMENTATION OF CYBERSECURITY STRATEGY

It is important for Ukraine's integration into the world community for it to continue implementing the strategy. The experience of advanced countries in the field of cybersecurity is key for Ukraine to avoid the negative consequences of the pandemic. However, it is important to take into account the poverty factor when implementing advanced information technologies

for the general population. It is also advisable to work on improving the system to eliminate problematic issues that have arisen in terms of its practical application. Authorities are encouraged to fix vulnerabilities in their systems, perform periodic data backups, actively scan all web applications for unauthorized access, improve cybersecurity with protections such as multi-factor authentication, and identify suspicious account activity and stop their access to systems.

•*Increasing the Success and Sustainability of Democracy and Governance Interventions in Post-Conflict Countries*, International Foundation for Electoral Systems, FES Report January 2022. The International Foundation for Electoral Systems (IFES) in February 2019 launched a project entitled the *Identifying Successful Democracy and Governance Approaches in Post-Conflict Countries.* Among the results of this project was an accurate assessment of the impact of democracy and governance assistance in post-conflict countries, using over 25 years of programming history by the *Consortium for Elections and Political Process Strengthening* (CEPPS). IFES was able to understand the specific mechanisms or interventions through which democracy and governance assistance providers can contribute to the improvement of democratic indicators, provide insights into the sustainability of intervention outcomes, and identify recommendations to mitigate or better navigate challenges and enhance the likelihood of interventions yielding successful or sustainable outcomes. Interventions whose gains were still seen and felt years after projects ended, and which drew more praise from partners, were those for which ownership

was quickly transferred to partners, those that were relatively easy or affordable to maintain, and those that permanently changed rules, practices and perceptions. These findings are particularly relevant in the field of democracy assistance in post-conflict, transitional environments, examples of which are (1) mitigation of commitment problems and uncertainty between stakeholders and increase in social cohesion across conflict lines, (2) support for decentralization of power and resilience to authoritarianism by building capacity of local authorities, (3) contribution to the transition of some armed groups into political parties, building the capacity of nascent parties and supporting the resolution of intergroup tensions, (4) contribution to women's empowerment by leveraging opportunities created by the disruption of power structures during conflict and transitions, (5) reduction of political violence by increasing the appeal of vote calculations and democratic competition, as opposed to violence, (6) reduction of electoral violence by consolidating democratic institutions that can provide a fair, non-violent path for political gains, reducing the need for protests and boycotts, (7) increasing the accountability of political institutions and actors by strengthening the capacity of civil society to hold them accountable, (8) increasing citizens' access to justice and respect for the rule of law, and (9) increasing local human capital and mitigation of the consequences of conflict-driven brain drain.

DISINFORMATION AND DEEPFAKES

In the upcoming third edition of **The ABA Cybersecurity Handbook**, scheduled for release and publication in early 2022, Matthew F. Ferraro and contributing author Suzanne E. Spaulding have provided a chapter entitled

Disinformation and Deepfakes: The Role for Lawyers and Law Firms, in which they focus on the threats and challenges of deepfakes, synthetic media and other forms of disinformation that target businesses and other private sector interests. The following approximately 12 pages of discussion was drawn directly from their chapter, with footnotes omitted, for which the authors provided their approval and permission, and for which we and ABA ROLI are most grateful.

DISINFORMATION SPREAD AT HIGHER SPEED

Contemporary public discourse, Ferraro and Spaulding write, is increasingly saturated by the age-old vice of disinformation, but the difference today is the speed with which online false information can spread, its scale and seeming veracity of forged images and audio, the credulity of those deluded by lies, resulting in what the authors call "the rise of mainstream conspiracism." While not just a political or social problem, the landscape of public falsehoods has grown since the January 6, 2021 siege of the U.S. Capital, from petty annoyances into dangerous threats to public health, civic peace, economic security and, ultimately, our democracy.

Disinformation now poses serious risks to businesses and the privacy sector through the weaponization of disinformation to harm brands, move markets, conduct fraud, and undermine trust in companies and industries. Deepfakes in the form of media created or manipulated by artificial intelligence (AI) is becoming more believable and more widely produced, according to Ferraro and Spaulding, who provide many examples of how synthetic media can supercharge viral conspiracies to harm corporate reputations, move stock

prices, target companies for fraud, steal business credentials, and much more.

ROLE OF LAWYERS AND LAW FIRMS

The critical roles played by lawyers and law firms will be part of the solution to find ways to confront the corrupted information environment and advise clients on preparatory and mitigatory actions in the face of disinformation about businesses and deepfakes targeting private-sector interests. Lawyers will also have to be cognizant of their unique ethical obligations as they serve society by strengthening the public's confidence in the rule of law and the administration of justice.

DISINFORMATION AND MISINFORMATION

Disinformation as the term is used in this context means "[t]he *deliberate* creation and distribution of information that is false and deceptive in order to mislead an audience," and includes information that may have a kernel of truth but is deliberately presented in a misleading manner, as is done with the knowing pushing of falsehoods with a specific intent, to influence others' perceptions.

This use of the term disinformation is distinct from misinformation, which while often used interchangeably with disinformation, also encompasses "[i]information that is false, though not deliberately; that is created inadvertently or by mistake."

ACTIVE MEASURES

Disinformation can also be a subset of "active measures," generally understood as "covert political operations ranging from disinformation campaigns to staging insurrections," the kind of information operations engaged in by the Soviet Union and others in the 20th century up until today by Russia and China. Such active measures are "not spontaneous lies by politicians, but the methodical output of large bureaucracies", nor need the pushed information be entirely false. Active measures may be in play when nation-states seek to harm private companies through disinformation campaigns designed to bolster favored businesses or national champions. but not all.

Deepfakes are a branch of AI, or artificial intelligence, that comes from a melding of two words: "deep learning" and "fake." Deep learning is a branch of AI that attempts to mimic the workings of the human brain in processing data.

Deepfakes are synthetic media (text, images, audio, or video) that are "either manipulated or *wholly generated* by AI." This technology provides the ability to manipulate and also create from whole cloth entirely false, believable media quickly and at scale. Think of Photoshop editing and Instagram filters on steroids.

FLAWLESS FORGERY

A deepfake can be a particularly realistic fake piece of media manipulated or created by computers, a flawless forgery so to speak, and in this context is

synonymous with “synthetic media” and “manipulated media.” As the technology used to make deepfakes gets better and more accessible, it can be applied to create fake digital maps or falsified images of overhead imagery used to track traffic at retail establishments, commodity inventories, real estate growth patterns and maps for traffic apps, just a few of the businesses that could be negatively impacted by such deepfakes.

The rapid increase in the number of online deepfakes is evident from analyses and studies that show a 6.82 % year-over-year growth rate of deepfake videos online, and a doubling of the number of deepfake videos on the internet every six months. This can lead to the ability of malign actors to create ever more convincing fake media showing people doing and saying things that did not occur in reality will be widespread.

DEEPFAKE COUNTERMEASURES

Deepfake countermeasures fall into two general categories. The first method attempts to detect phony media *after* it is created, as when an Israeli technology firm in July 2020 used deepfake-detection algorithms to reveal that the headshot employed by an author of op-eds in prominent Israeli newspapers was manipulated by AI and that the author himself was a “mirage.” Microsoft in September 2020 launched a program to assess media that provides a confidence score about whether that media has been manufactured artificially. The second method verifies photographs and other media at the “point of capture” in such a way that they cannot be altered or modified after the fact without leaving evidence of the manipulation.

THE LIAR'S DIVIDEND

There is a notable side effect of the propagation of deepfakes. The mere growth of believable synthetic media can foster the "liar's dividend," through which individuals successfully deny the authenticity of genuine media by claiming that the content is a deepfake. By leveraging skepticism about the authenticity of media to cast doubt on real evidence of their wrongdoing, liars will accrue a benefit or a dividend. An example of this was seen in the claims of former President Trump that the infamous *Access Hollywood* tape (in which he can be heard bragging about grabbing women by the p***y and sexually assaulting women) may be "fake."

THE ZEOLOT'S DIVIDEND

Also on the rise is a kind of "zealot's dividend," in which partisans who are not even the subjects of the media in question reject inconvenient media evidence that does not fit with their chosen narratives, claiming it is manipulated or synthetic. An example was seen with supporters of former President Trump dismissing as a "deepfake" a video of him conceding the 2020 election, and with political partisans claiming falsely that videos of President Joe Biden are deepfakes. The value of the liar's dividend and the zealot's dividends will grow dearer as more people learn about the quality and availability of this level of deepfake technology.

It is not beyond belief that foreign governments and organizations can also engage in disinformation campaigns against private business to bolster foreign companies or harm competitors. The Russian-backed TV and Internet channel RT America for the last few years has aired reports on the

dangers of 5G technology, linking 5G signals to brain cancer, infertility, and Alzheimer's disease, all claims that lack scientific support. Russia's goal appears to be to sow doubt about a technology that the United States believes is part of its future high-tech dominance.

BEST PRACTICES FOR MANAGING DISINFORMATION RISK: MODEL FOR UKRAINE?

Ferraro and Spaulding have identified the "Elite Eight" Best Practices for managing disinformation risk, and they emphasize that these are strategies on which businesses should work with their counsel to protect their brands and valuations from disinformation and deepfakes before as well as after companies are victimized.

(1) *Proactively Communicate an Accurate Positive Message*. Research shows that proactive messaging can establish strong defenses to disinformation. An April 2020 paper in the *HKS Misinformation Review* about COVID-19 disinformation makes this point. It reported that 87% of the public believed that handwashing and social distancing inhibit the spread of the coronavirus. The public accepted this truth because people had already absorbed messages about the efficacy of handwashing and social distancing in preventing the spread of the seasonal flu, the article argued. By contrast, it said that more than one in five people surveyed believed that Vitamin C was a remedy for the coronavirus in part because of longstanding misperceptions that Vitamin C cures the common cold. These findings suggest that, in the business context, a company should take steps to build brand

resilience[1]—to establish its messages in the public's mind early on, before disinformation starts spreading. If a company can construct stable public perceptions, it will be less likely to lose control of the narrative about its business to a barrage of bogus blogs and tendentious tweets.

(2) *Engage in Social Listening*. Companies need to understand how their brands are perceived on social media to get advance warning of any effort to spread disinformation. Law firms, cybersecurity consultancies, or public relations firms can be retained to do this work. Outside counsel can also consider retaining the third-party service providers directly; depending on the circumstances, their work may be entitled to legal privilege.

(3) *Conduct a Self-assessment*. Disinformation risk varies by company and circumstance. Businesses need to look in the mirror and ask, "What upcoming events carry the greatest risk? What aspects of the business are most vulnerable to attack? What messages would have the most resonance?" Preston Golson, a former CIA officer and now a director at the Brunswick Group, has called this "an audit of vulnerabilities." "In a world of complex tensions, organizations that take a position on a controversial issue, criticize the policies of a foreign government, or simply are on one side of a domestic political dispute, can end up being the subject of disinformation," he wrote. It is important that entities

understand these pressure points early. Furthermore, because, as noted above, disinformation and deepfakes pose special dangers of social engineering and impersonation, businesses should also assess their vulnerabilities to fraud and spearphishing.

(4) *Register Trademarks and Copyrights*. Because of the strong federal protection provided to intellectual property (IP), companies should work with counsel to register preemptively their trademarks, trade dress, and copyrights before they are manipulated by bad actors. If their IP is misused, copyright or trademark owners can bring lawsuits. Social media platforms also usually remove IP-infringing content if they receive a request from the IP's owner. For example, in 2019, anti-advertising activists uploaded to a social media platform a manipulated deepfake video of Kim Kardashian West appearing to say things she never did. *Vogue* magazine had posted the original video on which the deepfake was based a few weeks earlier, and because the copyright for that video belonged to *Vogue*, the magazine's publisher Condé Nast was able to lodge a copyright complaint against the manipulated video and have it taken down.

(5) *Make a Plan*. Many companies today work with attorneys to develop cybersecurity plans that anticipate cyber hacks and similar crises. Businesses need to expand their crisis planning to anticipate that reputational harm and disinformation may be a key objective of malicious actors. They need to prepare for fraud and social engineering by increasing training for team members (and expanding those who are

educated on these threats, to include professionals from communications, public relations, finance, and IT) and updating compliance and internal security protocols.

With regard to corporate reputations, entities cannot hope to design an effective response strategy after canards start to circulate. They need to prepare for such events the same way they should plan for cybersecurity breaches: by assigning specific responsibilities to members of an incident response team and running drills. Companies should also consider using technology to make videos of c-suite executives harder to manipulate.

(6) *Engage with Social Media Platforms*. If a company or its counsel see disinformation spreading online, it should contact the social media platforms being used to spread it and see if the information violates the platforms' Terms of Service. If so, the platforms may remove it.

(7) *Speak*. It can be a challenge to know when to directly address disinformation as opposed to ignoring it. There is a risk of amplifying false information that might otherwise fail to get traction. On the other hand, lies can travel remarkably fast and waiting too long can be costly. As part of their advance planning, companies should consider thresholds for taking specific steps, including when to speak directly to their customers, the media, and the public, as well as to third-party validators (who should be identified and contacted in advance as part of crisis planning). They should work with counsel to engage proactively

with regulators and file disclosures, as circumstances warrant.

(8) *If Necessary, Go to Court.* Free speech rights protect most opinions, but businesses are not defenseless when their brands are defamed or markets manipulated. For example, in early 2021, lies about fraud in the 2020 election led to high-profile civil actions against purveyors of disinformation. In one case, in February 2021, the voting software machine maker Smartmatic sued Rudy Giuliani and Sydney Powell, *Fox News* and individual *Fox* hosts, for their comments linking unfounded election fraud claims to Smartmatic. In March 2021, Dominion Voting Systems also sued *Fox News*, alleging similar claims. While the defendants maintain their innocence, and no court at this writing has ruled on the viability of these claims, the plaintiffs have already secured several favorable settlements and retractions in response to filing complaints.

NEED FOR AN INFORMED AND ENGAGED CITIZENRY

Beyond the direct implications for the practice of law, disinformation and deepfakes can threaten democracy in ways that lawyers may be uniquely suited to address. For example, the public skepticism generated by the "liar's dividend" can lead Americans to give up on trying to find the truth, or on the idea of truth altogether. And disinformation designed to undermine trust in institutions, including the courts, can accelerate disengagement from vital public institutions. Democracy cannot long function without an informed and engaged citizenry.

CONFIDENCE IN THE RULE OF LAW AND SYSTEM OF JUSTICE

Members of the bar can play an essential role in educating their communities and in helping to put out facts to dispel disinformation about specific cases or judges, or about the justice system as a whole. Attorneys have a vital responsibility, as recognized by the Model Rules of Professional Conduct, to serve as "public citizen[s]" with "special responsibility for the quality of justice" and to "further the public's understanding of and confidence in the rule of law and the justice system because legal institutions in a constitutional democracy depend on popular participation and support to maintain their authority."

ROLE OF LAWYERS IN DEALING WITH DISINFORMATION & DEEPFAKES

Ferraro and Spaulding provide ten takeaways in their final chapter on the role of lawyers in dealing with the evolving issues of disinformation and deepfakes.

(1) We live in an age of intensifying disinformation that poses significant, if often underappreciated, business and legal risks that attorneys need to address;

(2) Realistic manipulated media called deepfakes act as an accelerant to the negative trends of disinformation;

(3) Disinformation and deepfakes can cause significant private-sector harms, including hurting corporate reputations, facilitating fraud, enabling social engineering, manipulating markets, and causing personal harassment;

(4) Law firms, like any other business, are at risk from these dangers, too;

(5) Businesses should prepare now for the downsides of disinformation and deepfakes. While every company and situation is different, companies should consider several general principles around preparation, raising awareness, and communication;

(6) Lawyers have many important roles to play in dealing with these threats for themselves and their clients. Lawyers can help companies develop disinformation mitigation plans ahead of time, counsel clients when they are the subject to a viral conspiracy or a disinformation-enabled cyber hack, work with regulators, and go to court to vindicate a client's rights;

(7) Deepfake technology is not all bad, and the adoption of this technology for positive-use cases by more businesses, particularly in the entertainment and advertising sectors, is assured;

(8) Attorneys will be needed to help companies take advantage of these opportunities, from drafting contracts and licenses, to counseling on ethical uses, to advising on regulatory risk and helping to shape the legislative landscape, among others;

(9) Deepfakes pose unique challenges to litigators and courts. The rules of evidence require authentication standards that should, in theory, screen out manipulated media, but judges should prepare for dueling experts on the veracity of video and audio exhibits; and,

(10) Attorneys have professional, ethical, and legal obligations to serve the cause of justice by acting in a way that buttresses the public's confidence in the rule of law and the administration of justice, as well as the expertise and opportunity to counter the disinformation that threatens our democracy.

III. MODEL LAWS ON DATA PROTECTION

European Union model laws:

•Thomas Streinz, *The Evolution of European Data Law* (Oxford University Press 3rd ed. 2021). Streinz has provided a comprehensive overview of data protection and privacy enshrined in the EU's Charter of Fundamental rights. European data protection law has been globally diffused through extraterritorial application, conditional transfers of personal data, international agreements, and the EU's problematic retention of its role as global data regulator.

BRUSSELS EFFECT

European data protection law is widely seen as a key example of the Brussels Effect, a dynamic that leads to compliance with EU data protection laws by businesses outside the EU even when they are not legally required to do so. The underlying rationale of the Brussels Effect is that multinational businesses will act in this way in the face of regulatory demands across jurisdictions, rendering EU data law virtually inescapable due to its expanded jurisdictional reach. This is especially so in light of the

heavy cost of non-compliance caused by the GDPR's novel sanctions for non-compliance with EU law.

A problem arises, moreover, when one considers the U.S. CLOUD Act of 2018 and how it may ultimately diverge from the GDPR, making it difficult if not impossible to comply simultaneously with European data law and the data laws of the U.S. if companies are forced to differentiate their products by jurisdiction. An example of this divergence is where a U.S. electronic communication service provider is required to preserve, backup and disclose data within its possession, custody or control regardless of location, which at the same time the GDPR clearly mandates that administrative or judicial decisions by third countries are in themselves, in the absence of international agreements such as mutual legal assistance treaties, insufficient for a transfer of personal data from the EU to a third country. Under the CLOUD Act, a qualifying foreign government may enter into agreements with the U.S., in which case electronic communication providers can file a motion to quash orders that put them into a bind of violating one law or the other. In the absence of an EU-US agreement, companies in this predicament may not be able to comply with both the CLOUD Act and the GDPR at the same time.

EUROPEAN GOVERNMENTS' RELIANCE ON GOOGLE AND APPLE

When the COVID-19 Pandemic began to spread worldwide in spring 2020, European governments relied on Apple's and Google's infrastructural control over the operating systems on hundreds of millions of smartphones within Europe. These two global digital giants decided how *their* technology

could be used or not used for contact-tracing efforts by governments seeking technical solutions to a global public health crisis.

The Apple/Google episode shows the limitations of conventional data protection and privacy, especially when it was readily apparent that the Apple/Google solution was more privacy-preserving than what some European governments had preferred. Infrastructural control over data and resulting economic, social and political power exercised by global digital corporations remains largely unchecked by existing European data law. In practice much data regulation is determined by regulation through standards, software and infrastructure and structural forces, especially the concentration of data and infrastructural power in global digital corporations.

There is a difference between data regulation by law and by other means. In this context, data is a medium of governance, not just a regulatory object or an economic resource. As we enter a new era of data-dependent forms of governance, European data law will likely become of form of meta-regulation of legal governance by and with data.

• *Uniform Personal Data Protection Act*, Uniform Law Commission (National Conference of Commissioners on Uniform State Laws, 2021). The Uniform Personal Data Protection Act (UDPA) was approved and recommended by the Uniform Law Commission for enactment by all the

States in July 2021. The UPDPA is a model data privacy bill designed to provide a template for states to introduce to their own legislatures, and ultimately, adopt as binding law. The UPDPA would govern how business entities collect, control, and process the personal and sensitive personal data of individuals.

This model bill has been worked on since 2019 and includes the input of advisors, observers, the Future of Privacy Forum, and other stakeholders. The model bill is much narrower than some of the recent state privacy laws that have been passed, such as the California Privacy Rights Act and Virginia's Consumer Data Protection Act. Specifically, it would provide individuals with fewer, and more limited, rights including the right to copy and correct personal data. The bill does not include the right of individuals to delete their data or the right to request the transmission of their personal data to another entity. The bill also does not provide for a private cause of action under the UPDPA itself, but would not affect a given state's preexisting consumer protection law if that law authorizes a private right of action. If passed, the law would be enforced by a state's Attorney General.

APPLICATION OF UPDPA

The UPDPA would apply to the activities of a controller or processor that conducts business in the state or produces products or provides services purposefully directed to residents of this state and:
(1) during a calendar year maintains personal data about more than [a specified number] data subjects who are residents of this state, excluding

data subjects whose data is collected or maintained solely to complete a payment transaction;

(2) earns more than [x] percent of its gross annual revenue during a calendar year from maintaining personal data from data subjects as a controller or processor;

(3) is a processor acting on behalf of a controller the processor knows or has reason to know satisfies paragraph (1) or (2); or

(4) maintains personal data, unless it processes the personal data solely using compatible data practices.

PERSONAL DATA

The UPDPA defines "personal data" as a record that identifies or describes a data subject by a direct identifier or is pseudonymized data. The term does not include deidentified data. The bill also defines "sensitive data" as a category of data separate and apart from mere "personal data." "Sensitive data" includes such information as geolocation in real time, diagnosis or treatment for a disease or health condition, and genetic sequencing information, among other categories of data.

The law would not apply to state agencies or political subdivisions of the state, or to publicly available information. There are other carve-outs, as well.

DATA PRACTICES

The model bill also contains several different levels of "data practices," broken down into three subcategories:

(1) a compatible data practice;

(2) an incompatible data practice; and
(3) a prohibited data practice.

Each subcategory of data practice comes with a specific mandate about the level of consent required—or not required—to process certain data. For example, a controller or processor may engage in a compatible data practice without the data subject's consent with the expectation that a compatible data practice is consistent with the "ordinary expectations of data subjects or is likely to benefit data subjects substantially." Section 7 of the model bill lists a series of factors that apply to determine whether processing is a compatible data practice, and consists of such considerations as the data subject's relationship to the controller and the extent to which the practice advances the economic, health, or other interests of the data subject. An incompatible data practice, by contrast, allows data subjects to withhold consent to the practice (an "opt-out" right) for personal data and cannot be used to process sensitive data without affirmative express consent in a signed record for each practice (an "opt-in" right). Lastly, a prohibited data practice is one in which a controller may not engage. Data practices that are likely to subject the data subject to specific and significant financial, physical, or reputational harm, for instance, are considered "prohibited data practices."

The model bill has built in a balancing test meant to gauge the amount of benefit or harm conferred upon a data subject by a controller's given data practice, and then limits that practice accordingly.

UPDPA INTRODUCTION TO STATE LEGISLATURES JANUARY 2022: MODEL FOR UKRAINE?

After final amendments, the UPDPA will be ready to be introduced to state legislatures by January 2022. Versions of this bill can, and likely will be, adopted by several states over the next couple of years—and perhaps, eventually, lead to some degree of uniformity among the states' privacy laws.

•Benjamin E. Griffith and Sven Kohlmeier, *Data Protection, Privacy & Cybersecurity for Local Government,* International Municipal Lawyers Association 2020 Annual Conference, September 29, 2020.

The following Basic Cybersecurity Best Practices were identified during this presentation on data protection, privacy and cybersecurity for local government.

The cat-and-mouse game that seems to be taking place constantly between the perpetrators and victims of cybersecurity breaches, practices and measures is daunting. It has spawned a number of practices that can be implemented by municipalities to help protect their networks and systems. Some of these practices have been implemented by the private sector and are listed in a 2015 report from Online Trust Alliance (OTA). According to OTA, if the affected organizations and entities had implemented basic cybersecurity best practices, they could have prevented 90% of recent breaches. See Security & Privacy Best Practices (Jan. 21, 2015), https://otalliance.org/resources/security-privacy-best-practices.

OTA recommends all organizations implement these best practices:

1. Effective password management policies, using best practices for password management:

a. multi-factor authentication;

b. unique password for external vendor systems;

c. strong passwords comprised of an 8-character;

d. login abuse detection system monitoring connections, login counts, cookies, and machine IDs;

e. Avoid storing passwords;

f. Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure; and

g. Remove access immediately for any terminated employees or any third parties or vendors that no longer require access to your infrastructure.

2. Least privilege user access (LUA).3. Harden client devices by deploying multilayered firewall protections.

3. Conduct regular penetration tests and vulnerability scans of infrastructure.

4. Email authentication on all inbound and outbound mail streams.

5. Mobile device management program, requiring authentication to unlock a device, locking out a device after five failed attempts, using encrypted data communications/storage, and enabling the remote wiping of devices if a mobile device is lost or stolen.

6. Continuous monitoring in real-time the security of the organization's infrastructure.

7. Deploy web application firewalls to detect/prevent common web attacks.
8. Permit only authorized wireless devices to connect to the network.
9. Implement Always On Secure Socket Layer (AOSSL) for all servers requiring log in authentication and data
collection.
10.Review server certificates for vulnerabilities and risks of domains being hijacked.
11.Develop, test, and continually refine a data breach response plan

STRATEGIC LITIGATION AGAINST PUBLIC PARTICIPATION

The proliferation of SLAPP laws:

•*SLAPP in the EU Context*, EU Citizen, Academic Network on European Citizenship Rights, May 29, 2020. This report highlights the challenges to freedom of expression and European democracy, with an analysis of the legal and non-legal tools used in a SLAPP-related context. SLAPP cases interfere with the values of a free and functional press, especially investigative journalism. SLAPPs, Strategic Lawsuits Against Public Participation, are groundless or exaggerated lawsuits and other legal forms of intimidation initial by state organs, business corporations and individuals in power against weaker ones – journalists, civil society organizations, human rights defenders and others – who express criticism or transmit messages uncomfortable to the powerful, on a public matter. The aim of a SLAPP suit is not to win the case but instead the procedure is initiated for the sole reason of having the procedure, in an attempt to intimidate, tire out, and consume the financial and psychological resources of the speakers, with the ultimate goal of achieving a chilling effect and silencing them,

which will also discourage other potential critics from expressing their views.

Just as a free and functional press, especially investigative journalism, is a cornerstone of all democracies, it is also a basic pillar of European integration. SLAPP cases interfere with these values and prevent citizens from engaging in a meaningful debate on public issues. SLAPP cases also interfere with fundamental rights of individuals, such as freedom of expression and freedom to receive information. The common European rules are based on the mutual trust between Member States. In case of tort damages claims, a plaintiff may choose the jurisdiction flexibly. The choice of law rules made an exception to defamation cases; therefore, plaintiffs have extensive choice of applicable law. As there are significant differences in both the procedural and substantive rules of defamation among Member States, vexatious litigants are able to leverage the legal regime to their advantage and against public participation. At stake in SLAPP suits is the very concept of European or American Democracy and fundamental rights. SLAPP actions attack democratic public participation, and they indirectly threaten the democracy and the rule of law within the European Union.

RULE OF LAW OVERSIGHT BY EU

Tolerating or getting involved in SLAPP cases by the government should be regarded as early warning signs for a rule of law oversight by the EU. A rule of law oversight should register reported SLAPP-cases, and also eventual abuse of antiSLAPP.

On 19 April 2018, the European Parliament passed a resolution on the "Protection of investigative journalists in Europe: the case of Slovak journalist Ján Kuciak and Martina Kušnírová". One of the points of resolution called on the European Commission and the EU Member States to "present legislative or non-legislative proposals for the protection of journalists in the EU who are regularly subject to lawsuits intended to censor their work or intimidate them, including pan-European antiSLAPP (Strategic Lawsuit Against Public Participation) rules".

The European Commission has variously addressed the question of SLAPP suits and anti-SLAPP legislation in the EU. In response to written questions prior to her confirmatory hearing before the European Parliament, Vice President-designate for Values and Transparency Jourová stated that "The issue of Strategic Lawsuits Against Public Participation (SLAPP) can be considered as an abuse of defamation laws. In particular, I am aware that such lawsuits can amount to a misuse of the law which makes it possible to threaten journalists with lawsuits that would be too expensive to fight –even in cases where the lawsuits have little or no chance of succeeding –which can create a chilling effect and are therefore a threat to media freedom. I therefore consider that this issue is of direct relevance to my portfolio and the combination of questions at the intersection of private international law, public policy and media freedom deserve deeper analysis".

In her previous capacity as Commissioner of Justice and Consumers, Commissioner Jourová responded to a question from an MEP on national

anti-SLAPP legislation, stating that "[i]n the absence of Union competence to harmonise substantive defamation laws and address SLAPP lawsuits, Member States are free to introduce such legislation at national level", but that such legislation will have to be in line with relevant EU laws, including issues of jurisdiction of Member States' courts in cross-border civil and commercial disputes and of the recognition and enforcement of judgments from other Member States.

•Lauren Merk*, Strategic Suits Against Public Participation in the Age of Online Speech: The Relevance of Anti-SLAPP and Anti-CyberSLAPP Legislation,* University of Cincinnati Intellectual Property and Computer Law Journal, Vol. 5, Issue 1, 2020. This article provides an overview of the recently coined "cyberSLAPPs" and relevant anti-SLAPP legislation in the digital age. SLAPPs are often associated with defamation or libel claims, but not all are related to speech.

The term "cyberSLAPP" is sometimes used to refer to SLAPPs that infringe on individuals' First Amendment rights on the internet. SLAPPs arising from blog posts and online comments are among the examples of cyberSLAPPs that the American Civil Liberties Union ("ACLU") of Ohio offers on its website. The ACLU of Ohio explains that oftentimes, cyberSLAPPs not only seek to intimidate online speakers, but also to uncover the speaker behind anonymous internet speech. These concerns raise questions about the right to speak anonymously on the internet, First Amendment protections to online speech, and whether protections similar to reporters privileges may apply to ordinary internet commentary.

There is currently no federal anti-SLAPP law, and consequently, no federal anti-cyberSLAPP statute. However, some case law exists regarding whether states' anti-SLAPP legislation also protects against cyberSLAPPs.
Exercising one's First Amendment rights to free speech and participation is arguably easier than ever with the rise of the internet and online forums.

The internet has undoubtedly impacted the accessibility and ability for private individuals to exercise their First Amendment rights of speech and participation. As the Public Participation Project noted, "[t]echnology now makes it possible for everyone to don the hat of journalist, editor, town crier or anonymous pamphleteer." While this change in the public participation landscape raises the possibility of increased participation, it also presents new legal challenges and questions. Further, the increase in speech and participation means that more individuals may find themselves vulnerable to SLAPP suits. As such, strategic lawsuits against public participation are relevant to internet law.
The right to public participation has long been a cornerstone of American democracy, and continuous developments to the internet provide brand new ways in which individuals can exercise their First Amendment rights. As public participation and exercising speech becomes easier than ever, there are new opportunities for litigants to bring meritless SLAPP claims against defendants.

While many states have enacted anti-SLAPP laws to help protect against and discourage SLAPPs, the levels of protection that anti-SLAPP laws provide vary greatly by state. Some states, like California, offer broad

protections for SLAPPed defendants. Other states, like Pennsylvania and New York, have narrower statutes that apply to SLAPPs resulting only from certain forms of participation. An anti-SLAPP statute like that of Minnesota may have aggressive provisions that go so far as to lose effectiveness, or even be determined unconstitutional. Other states, like Virginia, may be trying to actively amend existing anti-SLAPP laws.

Finally, some states lack any anti-SLAPP legislation at all. The lack of a comprehensive federal anti-SLAPP statute presents multiple questions and concerns. For instance, federal courts are split in regard to the applicability of state anti-SLAPP laws in federal courts. While there has been a call for a federal anti-SLAPP statute as well as multiple attempts to pass such legislation in recent years, a federal anti-SLAPP law has not yet resulted.

•Tyler J. Kimberly, *A SLAPP Back on Track: How Shady Grove Prevents the Applications of Anti-SLAPP Laws in Federal Courts,* Case Western Reserve Law Review, Vol. 65, Issue 4, 2015. The U.S. Supreme Court's plurality decision in *Shady Grove Orthopedic Associates v. Allstate Insurance Company* established that (1) a federal rule can be limited where Congress passes legislation to do so, (2) anti-SLAPP statutes are preempted by the Federal Rules of Civil Procedure, (3) such statutes cannot apply in federal court since they are in conflict with the Federal Rules, (4) nor can an anti-SLAPP motion to dismiss be heard in federal court. *Shady Grove* gave

sweeping authority to the FRCP in the face of possibly conflicting state laws. The Federal Rules are thus given a textual interpretation, and absent an Act of Congress or language in the rule itself, state law cannot limit the rule.

•Katelyn E. Saner*, Getting SLAPP-ED in Federal Court: Applying State Anti-SLAPP Special Motions to Dismiss in Federal Court after Shady Grove,* Duke Law Journal, Vol. 63, 2013. This article analyzes *Shady Grove* and whether it should apply to state level anti-SLAPP special motions to dismiss should be applied in federal courts sitting in diversity. Absent intervention by Congress to adopt a federal anti-SLAPP statute, the answer is no.

•Andrew I. Roth*, Upping the Ante: Rethinking Anti-SLAPP Laws in the Age of the Internet,* BYU Law Review Vol. 2016, March 2016. This article looks at the expansion of anti-SLAPP statutes in the context of internet defamation. The expansion of anti-SLAPP to public speech, particularly on the internet, presents a dilemma for lawmakers: should they protect the rights of petition and free speech from increased threats of chilling, or should they protect defamation victims who are at a significantly greater risk of harm from online libel? It has upped the ante for anti-SLAPP laws to be expanded into the realm of internet defamation and libel, and the stakes for speakers and those who they speak about have risen significantly.

•*The Use of SLAPPS to Silence Journalists, NGOs and Civil Society,* Policy Department for Citizens' Rights and Constitutional Affairs, June 2021. This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the JURI Committee, and provides an analysis of legal definitions of Strategic Lawsuits Against Public Participation (SLAPP) and

assesses the compatibility of anti-SLAPP legislation with EU law.
It is recommended that an anti-SLAPP Directive should be adopted, and that the Brussels Ia Regulation and Rome II Regulation should be recast to limit the incidence of SLAPPs.

The European Convention on Human Rights establishes a positive obligation to safeguard the freedom of pluralist media and to 'create a favorable environment for participation in public debate'. Strategic Lawsuits Against Public Participation (SLAPP), a form of retaliatory lawsuit intended to deter freedom of expression on matters of public interest, constitute a significant threat to the fulfilment of this obligation. By restricting scrutiny of matters of public interest, whether of economic or political concern, SLAPPs also have a deleterious effect on the functioning of the internal market, as well as the rule of law in the European Union. However, while several jurisdictions outside the European Union have adopted antiSLAPP legislation, no Member State of the Union has yet done so. Nor has the EU itself yet adopted any legislation which would dissuade the institution of SLAPPs. There is therefore a significant gap in the integrity of the legal order of the Union. In 2021, the Council of Europe's Commissioner for Human Rights observed that, while SLAPPs are not a new phenomenon, the extent of the problem is increasing and poses a substantial threat to freedom of expression.

There is therefore a need for robust legislative intervention in the European Union with a view to stemming the flow of litigation which is intended to suppress public participation in matters of public interest. While legislative

models adopted in the United States, Canada and Australia are instructive insofar as the overarching structure of EU legal reform is concerned, EU legislation would require the careful articulation of bespoke definitions and methods of analysis. This should be characterized by a distinctive approach which draws on good practice from jurisdictions outside the European Union, but which recognizes nevertheless the unique characteristics of the EU legal order and the legal traditions of its Member States.

Furthermore, legislative intervention must be formulated in a manner which empowers national courts to attain the intended outcome of expeditious dismissal of cases without harming potential claimants' legitimate rights to access courts. Properly framed anti-SLAPP legislation affords the claimant the opportunity to present legitimate claims to the court and therefore satisfies the requirements of Article 6 ECHR. Far from stultifying access to courts for the parties, anti-SLAPP legislation would dissuade the misuse of civil procedure in a manner which prevents respondents from articulating a defense in accordance with EU law and international human rights instruments.

In addition to the adoption of an anti-SLAPP Directive, it is recommended that the Brussels Ia Regulation concerning jurisdiction, recognition and enforcement of judgments be recast with a view to adopting a specific rule concerning defamation claims, and thereby to distinguish jurisdiction in defamation cases from ordinary torts. This would restrict the availability of opportunities for forum shopping arising from the Regulation as presently

framed. To this end, it is recommended that jurisdiction should be grounded in the forum of the defendant's domicile, unless the parties agree otherwise. This would enable public interest speakers to foresee where they will be expected to defend themselves, and would be in keeping with the core values of the Brussels Ia Regulation, namely predictability and the limitation of forum shopping.

Greater predictability as to the outcomes of choice of law processes is also needed to dissuade meritless litigation intended to suppress public participation. Accordingly, it is recommended that a new rule be included in the Rome II Regulation which would harmonize national choice of law rules in defamation cases. It is proposed that this rule should focus in the first instance on the closest connection with the publication and its audience, namely the law of the place to which the publication is directed.

•*Proposal for an EU Anti-SLAPP Directive*, Human Rights Centre Ghent University and Legal Human Academy, December 2, 2020. A model EU anti-SLAPP directive was released on December 1, 2020, an initiative of a broad network of NGOs supporting the advocacy and initiatives for anti-SLAPP legislation at the level of the EU. The model for an EU anti-SLAPP Directive proposes a set of rules that should guarantee that in each EU country, SLAPPs can be dismissed at an early stage of the proceedings, that SLAPP litigants pay for abusing the law and the courts, and that SLAPP targets are given assistance to defend themselves. The Directive also contains provisions against "libel tourism" and includes protection of public watchdogs such as journalists, human rights defenders, NGOs, activists,

and whistle-blowers that help hold the powerful to account and keep the democratic debate alive.

•Dr. Justin Borg Barthet, *Advice Concerning the Introduction of Anti-SLAPP Legislation to Protect Freedom of Expression in the European Union*, Centre for Private International Law, May 19, 2020. This article provides an overview of several jurisdictions within the EU that retain problematic rules of evidence and lack tools which would dissuade vexatious litigation and threats thereof. This is especially problematic in the context of sophisticated financial crime and other activities where the suppression of evidence of wrongdoing is a central feature of relevant activity. The European Union is called upon to either (1) introduce legislation to harmonize the rules of evidence in defamation cases, for which it has competence as a consequence of the importance of journalistic revelations in the integrity of an internal market governed by the rule of law, or (2) if this proves politically impossible, to adopt coordinating measures which in response to the preservation of press freedoms and the rule of law, and to follow these up with well-publicized monitoring.

•David L. Hudson, Jr., *Anti-SLAPP Coverage and the First Amendment: Hurdles to Defamation Suits in Political Campaigns*, American University Law Review, Vol. 69, Issue 5, 2020. This articles addresses how First Amendment protection is at its zenith when speakers engage in political speech, as in speech about political candidates, which is inherently political speech. Defamation suits that arise out of political campaigns face significant hurdles and obstacles, including (1) anti-SLAPP laws and a greater public awareness of SLAPP suits; (2) a history and tradition of

mudslinging and enhanced protection of political speech during political campaigns; and (3) the First Amendment-inspired doctrine of rhetorical hyperbole.

The negative essence of SLAPP suits was colorfully described by a New York state court judge in a 1992 decision:

"SLAPP suits function by forcing the target into the judicial arena where the SLAPP filer foists upon the target the expenses of a defense. The longer the litigation can be stretched out, the more litigation that can be churned, the greater the expense that is inflicted and the closer the SLAPP filer moves to success. The purpose of such gamesmanship ranges from simple retribution for past activism to discouraging future activism. Needless to say, an ultimate disposition in favor of the target amounts to a pyrrhic victory. Those who lack the financial resources and emotional stamina to play our the "game" face the difficult choice of defaulting despite meritorious defenses or being brought to their knees to settle. The ripple effect of such suits in our society is enormous. Persons who have been outspoke on issues of public importance targeted in such suits or who have witnessed such suits will often choose in the future to stay silent. Short of a gun to the head, a greater threat to First Amendment expression can scarcely be imagined." *Gordon v. Marrone*, 590 N.Y.S, 2d 649, 656 (N.Y. Sup. Ct. 1992).

Online speech that exaggerates, distorts, and paints a less than complete picture is not only a problem but can become a vast breeding ground for defamation. Defamation law serves an important purpose and reflects no more than our basic concept of the essential dignity and worth of every

human being, in the words of Justice Potter Stewart in *Rosenblatt v. Baer*, 383 U.S. 75, 92 (1966) (Stewart, J., conc. op.).

In the social media age, speech has exploded, as had defamation. But the prevalence of anti-SLAPP laws, the judicial protection afforded to political speech, and the defense of rhetorical hyperbole combine to make it very difficult to recover for defamation arising out of social media posts during political campaigns. At that juncture when political speech receives the greatest among of First Amendment protection, the doctrine of rhetorical hyperbole will protect much unsavory, loose, uncivil, figurative, exaggerated and repugnant language that often characterizes political campaign speech, and for that reason recovery of monetary damages by a candidate is highly unusual.

CRIMINAL INVESTIGATIONS WITHOUT ONLINE SAFEGUARDS

The dilemma of criminal investigations without adequate safeguards online for the protection of freedom of speech and expression, access to information, and rights to privacy:

•Kaplina Oksana & Sharenko Svitlana, *Access to Justice in Ukrainian Criminal Proceedings During the COVID-19 Outbreak*, Access to Eastern Europe Issue 2/3 (7) 2020. This article examines relevant issues of criminal proceedings in the context of the COVID-19 pandemic in Ukraine, during which many governments focused their efforts on protecting democratic values and ensuring not only the rights and legitimate interests of their people, but also their lives and health.

CEPEJ: MODEL FOR UKRAINE?

The pandemic affected not only the economies of many countries, but also had a great impact on their democratic development and fundamental rights, matters that have always been a priority of any democratic society in which the rights and legitimate interests of those seeking judicial protection under the rule of law are respected. The Council of Europe for the Efficiency of Justice (CEPEJ) has gained high importance during this period as the COE developed tools for the member states to address problems of ensuring access to justice in the pandemic.

BEST PRACTICES

The widespread discussion of such experiences is useful for member states as they seek to improve existing legislation that takes into account best practices. Specifically, during a pandemic there are certain restrictions that are necessary measures to preserve the health and life of the population, while at the same time emergency measures must be based on the fundamental principles of the rule of law, legality, legal certainty and proportionality, and must be sufficient in case of danger and must be accompanied by a reasonable number of guarantees against the arbitrariness of the authorities.

AMENDMENTS NEEDED TO THE CPC OF UKRAINE

When considering the importance of restricting the constitutional human right to liberty and security of one's person, the authors of this article, Oksana and Svitlana, make a strong case for amending and revising the Criminal Procedure Code (CPC) of Ukraine, embodied in the CPC of

Ukraine: Law of Ukraine of 13April 2012, No. 817-IX, and amendments to the CPC of Ukraine of 3August 2020, No. 540-IX. These changes and further amendments would apply to the extension of detention which may take place by videoconference, but with the addition of a system of guarantees of voluntary consent of the suspect or accused, in order to lessen or mitigate the automatic continuation of a most severe precautionary measure. These changes would also extend to the creation o fan effective mechanism for judicial control over the rights, freedoms and legitimate interests of persons in criminal proceedings as well as the creation of a system of guarantees of reasonable terms of criminal proceedings in a pandemic.

GDPR TRIGGERS DOMINO EFFECT OF U.S. DATA PRIVACY LAWS

•Elizabeth Field, *United States Data Privacy Law: The Domino Effect After the GDPR* (UNC School of Law, North Carolina Banking Institute, March 1, 2020). The domino effect described in this post-GDPR article reflects the stateside efforts of California, then New York and then several other states to adopt their own SHIELD versions of data privacy and consumer protection laws. With more states enacting consumer protection rights and strict data privacy policies in recent years, the financial industry will either need to accept these new compliance challenges and stricter regulations or begin to play an active role in the data privacy debates. The GDPR was the first such law to have far-reaching and extensive consequences for U.S. financial services companies, and California led the way stateside. Other states, including New York and Hawaii, also enacted GDPR-like legislation, further continuing the trend. Future consumer protection legislation could continue to extend its regulations to financial

entities, thus mirroring the EU law. As new state data privacy laws begin to take effect, unexpected costs, regulatory issues, and enforcement impossibilities may continue posing compliance challenges for financial organizations, large and small.

DATA PRIVACY LAWS AT STATE LEVEL

While state legislatures continue to introduce new data privacy laws, Congress has been considering its own federal reform, the initial blueprint for which was laid out by the Obama Administration in the form of the Consumer Privacy Bill of Rights, which included what were termed the "Fair Information Practice Principles. This initiative recognized the importance of individual consumer protection rights, including knowing how one's data is "collected, used, and shared by companies and government entities alike." Over time, the Obama proposal lost momentum, and the Trump Administration focused very little on technology policy. By 2019, some members of Congress began discussing the need to create a unified, federal data privacy law. With California's CCPA soon to take effect, Republicans and Democrats recognized the need for a comprehensive federal law to protect consumer privacy. This approach sprung from the inconsistent patchwork approach taken by the United States, compared to other similarly developed countries which implemented overarching privacy regimes incorporating the EU's GDPR. As more state legislatures pass data privacy laws, the need for federal regulation only increases. Nonetheless, a unified and comprehensive federal data protection policy could possibly wreak havoc on financial institutions that utilize complicated systems for processing customer information. According

to the NCSL, at least 38 states have introduced more than160 consumer privacy related bills in 2021, and comprehensive privacy legislation was the most common type of bill, introduced in at least 25 states. Comprehensive legislative in this context means laws that are similar to the CCPA, i.e., broadly regulating the collection, use and disclosure of personal information and providing an express set of consumer rights with regard to collected data, such as the right to access, correct and delete personal information collected by businesses.

IV. RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

Protection of personal data

•*Ukraine: Partly Free*, Freedom House 62/100,

This is the Freedom House annual report on Ukraine, highlighting conventions for the protection of individuals with regard to automatic processing of personal data. The FH report's numerical scores and listing of status do not reflect conditions in the occupied Ukrainian territories of Crimea and Eastern Donbas. This report does assess the level of political rights and civil liberties in a given geographical area, regardless of whether they are affected by the state, nonstate actors, or foreign powers. Disputed territories are sometimes assessed separately if they meet certain criteria, including boundaries that are sufficiently stable to allow year-on-year comparisons.

POSITIVE REFORMS AND EFFORTS TO COMBAT CORRUPTION

Ukraine has enacted a number of positive reforms since the protest-driven ouster of President Viktor Yanukovych in 2014. Corruption remains

endemic, however, and the Ukrainian government's initiatives to combat it have met resistance and experienced setbacks. Attacks against journalists, civil society activists, and members of minority groups are frequent, and police responses are often inadequate. Russia occupies the autonomous Ukrainian region of Crimea, which it invaded in the aftermath of Yanukovych's ouster, and its military supports armed separatists in the eastern Donbas area.

KEY DEVELOPMENTS IN UKRAINE DURING 2020

- More than one million people tested positive for COVID-19, and 18,533 people died during the year. Though the government imposed restrictions on movement and public space, most measures were deemed to be proportionate.
- In October 2020, multiple reports alleged that the head of the Constitutional Court, Oleksandr Tupytsky, had obtained land in occupied Crimea, failed to declare luxurious real estate in Kyiv, and was linked to a prominent case of judicial fraud.
- In October, the Constitutional Court annulled multiple anticorruption laws that required the public declaration of government officials' and representatives' assets and mandated criminal punishments for not doing so. Multiple judges who published their financial holdings had been under investigation because of these laws.
- During November and December, President Volodymyr Zelenskyy attempted to dissolve the Constitutional Court after it annulled significant anticorruption legislation. Though the Court was not

dissolved, the parliament passed new, albeit weakened legislation replacing the annulled anticorruption measures.

MIXED ELECTORAL SYSTEM FOR PARLIAMENT

The mixed electoral system for the Ukrainian parliament that has governed past polls, including those in 2019, has been criticized as prone to manipulation and vote-buying. President Zelenskyy attempted to introduce an entirely party list–based system prior to the 2019 parliamentary election, but could not garner enough parliamentary support. However, in December 2019, the new parliament adopted an electoral code that partially implemented a proportional representation voting system, with open party lists for both parliamentary and local elections, and Zelenskyy enacted it at the end of the year.

In October 2020, the Central Election Commission decided not to conduct local elections in 18 communities of the Donetsk and Luhansk regions in eastern Ukraine, located close to the contact line with noncontrolled territories. The decision affected 475,000 voters, who continued to be governed by military-civil administrations, which are appointed directly by the president.

DYNAMIC COMPETITION AMONG PARTIES

Ukrainian politics feature dynamic competition among parties. Opposition groups are represented in the parliament, and their political activities are generally not impeded by administrative restrictions or legal harassment. Generally, grassroots parties have difficulty competing with more

established parties that enjoy the support and financial backing of politically connected business magnates, known as oligarchs.
In the second election round held in April 2019, Zelenskyy won the presidency by a large margin, defeating incumbent president Poroshenko. In July's elections, President Zelenskyy's new Servant of the People's party took an absolute majority of seats in the Rada, defeating the incumbent European Solidarity grouping.

RUSSIAN INFLUENCE IN UKRAINIAN POLITICS DECLINING

Russian influence in Ukrainian politics has continued to decline since Yanukovych's ouster, though Moscow retains influence in some eastern and southern regions. Ukraine's oligarchs exert significant influence over politics through their financial support for various political parties, and lobby for the appointment of loyalists to key institutional positions.
Although electoral laws forbid the use of public resources in election campaigns, incumbent officials used administrative resources during the local election campaign, while law enforcers turned a blind eye to the practice.

POLITICAL PARTICIPATION OF WOMEN AND MINORITY GROUPS

There are no formal restrictions on the participation of women and members of ethnic, racial, or other minority groups in political life. However, their voting and representation are hindered by factors including discrimination that discourages their political participation, the conflict in the east, lack of identity documents for many Roma, and rules against running as an independent for many local, district, and regional offices. Internally

displaced persons (IDPs), of which there are over 1.5 million, face legal and practical barriers to voting. Societal discrimination against LGBT+ people affects their ability to engage in political and electoral processes.
The Law on Local Elections mandates a 30 percent quota for women on party lists, but it is not effectively enforced. A record 87 women were elected to parliament in 2019, though this amounts to only 20 percent of all seats.

REFORM MEASURES IMPLEMENTED BY ELECTED OFFICIALS

Elected officials craft and implement reforms, though many initiatives stall due to opposition from powerful business groups and other special interests. The main obstacle to effective governance in government-controlled parts of Ukraine is corruption.

ANTI-CORRUPTION EFFORTS CONSISTENTLY NEEDED

Corruption remains a serious problem, and even the little remaining political will to fight it is eroding, despite strong pressure from civil society. Anticorruption agencies have repeatedly been ensnared in politically fraught conflicts with other state entities and elected officials. In September 2020, the Constitutional Court ruled that a prominent anticorruption agency created by the ruling party was unconstitutional and shut down multiple investigations that had been opened by the agency. The agency had been investigating multiple sitting judges. The High Anti-Corruption court, created in September 2019, convicted 16 high-ranking officials in 2020.
In October 2020, multiple reports claimed that Constitutional Court Chief Justice Oleksandr Tupytsky allegedly had illegally obtained and owned land in Russia-occupied Crimea, omitted recording his luxurious real estate in

Kyiv among his assets, and had ties to a prominent case of judicial fraud. Tupytsky denied any wrongdoing. The State Bureau of Investigation opened a criminal investigation alleging that Tupytsky had committed treason by owning land in Russian-occupied Crimea.

PROGRESS ADVANCING TRANSPARENCY

In previous years, Ukraine made some progress in advancing transparency, for example by requiring that banks publish the identity of their owners, and by passing a 2016 law obliging politicians and bureaucrats to file electronic declarations of their assets. However, in October 2020, the Constitutional Court annulled the asset-declaration law, as well as a law that dictates criminal punishments for falsified asset reporting. Law enforcement agencies were forced to close some high-level corruption cases and remove the full database of official declarations from public access. Parliament reinstated a weakened version of the law in December.
In July 2020, the director and several high-ranking officials of the National Bank, a historically independent regulator, resigned due to systemic political pressure and the installation of a presidential loyalist as the bank's new leader.

PUBLIC PROCUREMENT PROCESS CENTRALIZATION NEEDED

After making progress to enhance the accessibility of information about public procurements in recent years, Ukraine failed to set up a centralized system about the purchasing medical equipment—including vaccines—to fight the coronavirus pandemic in a timely and transparent manner. Moreover, the Finance Ministry reported in December that about 26 percent

of the money allocated to the COVID-19 emergency fund was spent on building roads.

CONSTITUTIONAL FREEDOMS OF SPEECH AND EXPRESSION

The constitution guarantees freedoms of speech and expression, and libel is not a criminal offense. The media landscape features considerable pluralism, and open criticism of the government and investigation of powerful figures. However, business magnates own and influence many outlets, using them as tools to advance their agendas. President Zelenskyy has received significant support from media outlets controlled by banking magnate Igor Kolomoisky. Other parties also receive favorable coverage from "friendly" media. Zelenskyy at times has also refused to take reporters' questions, and his staff has occasionally refused access to spaces journalists are legally permitted to enter.

BAN ON RUSSIAN SOCIAL MEDIA

A number of Russian news outlets and their journalists are prohibited from entering the country. Various language laws impose upon news outlets requirements that certain content be in the Ukrainian language. In April 2020, the National Security Council and President Zelenskyy extended a ban on Russian social media in Ukraine.

THREATS OF VIOLENCE AND INTIMIDATION VS. JOURNALISTS

Journalists continued to face threats of violence and intimidation in 2020, and Ukraine's courts and law enforcement agents often fail to protect their rights. In August, several international media watchdogs urged Ukrainian

authorities to investigate the torching of a car affiliated with an investigative television program and the alleged surveillance of its journalists. By the end of the year, the police reportedly had identified three suspects.

MEDIA FREEDOM VIOLATIONS

The independent Institute of Mass Information recorded 205 media-freedom violations in 2020, including 19 cases of physical violence, 11 cyberattacks, 111 incidents of interference, 18 incidents of threats, 17 cases of restricting access to public information, and 2 cases of direct censorship. The National Police initiated 200 investigations of various crimes against journalists in 2020.

REINVIGORATION OF CIVIC GROUPS

Numerous civic groups emerged or were reinvigorated following the departure of Yanukovych in 2014, and many are able to influence decision-making at various levels of government. In 2019, the Constitutional Court struck down a law that had required leaders, staff, and contractors of nongovernmental organizations (NGOs) focused on corruption to submit asset and income declarations. Populist lawmakers had used the information made public through the law to smear the groups as working to harm Ukraine on behalf of malicious "foreign agents."

GROWING THREATS OF VIOLENCE VS NGOs

However, in recent years, NGOs have faced growing threats of violence, and those responsible are rarely brought to justice. In July 2020, the house of

Vitaliy Shabunin, head of the board of the Anti-corruption Action Centre, was set on fire. The police started a criminal investigation but had no suspects by the end of the year.

Ukraine has long suffered from corrupt and politicized courts, and recent reform initiatives aimed at addressing the issue have stalled or fallen short of expectations.

In October 2020, President Zelenskyy attempted to dissolve the Constitutional Court after it annulled laws aimed at fighting corruption; multiple Constitutional Court judges had been under investigation because of those laws. Shortly thereafter, the State Bureau of Investigation opened a criminal case against several Constitutional Court judges for allegedly attempting to seize state power. Though he was unable to dissolve the body, Zelenskyy ordered by presidential decree in December the suspension of Constitutional Court Chief Justice Oleksandr Tupytsky, who was also being investigated for bribery and witness tampering. The court claimed that Tupytsky's suspension was unconstitutional, though it then opened an inquiry into removing him from his position. The crisis was unresolved at year's end.

PROSECUTION FOR CRIMINAL WRONGDOING

Although due process guarantees exist, in practice individuals with financial resources and political influence can escape prosecution for wrongdoing. According to statistics from the World Prison Brief published in April 2020, about 37 percent of prisoners are in pretrial detention.

The government has made little progress in meeting domestic and international demands to investigate and prosecute crimes committed during the last months of the Yanukovych administration in late 2013 and early 2014, which included the shooting of protesters.

Judges consistently move to stymie corruption investigations into high-profile officials, including within the judiciary. In September and October 2020, the Constitutional Court annulled a series of anticorruption laws that required asset declarations of public officials, created anticorruption institutions, and empowered key anticorruption actors. The National Anticorruption Bureau and the National Agency for Prevention of Corruption reportedly were forced to close multiple ongoing investigations because of the ruling.

NATIONAL ANTICORRUPTION BUREAU

In December 2020, the National Anticorruption Bureau complained about the presidentially appointed prosecutor general's "unprecedented meddling" in the investigation of a bribery case related to deputy head of the president's office.

STABLE SECURITY STATUS

The security situation is generally stable outside of the occupied areas. However, there have been a number of high-profile assassinations and assassination attempts in recent years, some of which targeted political figures. Conditions in many prisons are squalid and dangerous.

PROHIBITED DISCRIMINATION AGAINST MINORITIES/LGBT+

A 2012 law introduced a nonexclusive list of grounds on which discrimination is prohibited. Gender discrimination is explicitly banned under the constitution. However, these protections are inconsistently enforced, and the Romany minority and LGBT+ people experience significant discrimination in practice. Roma and LGBT+ people and groups generally only receive police protection or justice for attacks against them when there is intense pressure from civil society or international observers. Rights groups have reported that employers openly discriminate on the basis of gender and age.

FIGHTING DOMESTIC ABUSE

In September 2020, President Zelensky signed a decree aimed at creating a network for fighting domestic abuse, citing a spike in domestic violence in the first half of the year as a result of a nationwide lockdown.

PERSONAL AUTONOMY AND INDIVIDUAL RIGHTS

Freedom of movement is generally not restricted in areas under government control. Ukraine's cumbersome system requiring individuals to be legally registered at an address to be able to vote and receive some services, however, creates a barrier to full freedom of movement, in particular for the displaced and those without an address where they could be registered for official purposes.

MOVEMENT RESTRICTIONS DURING PANDEMIC

Movement restrictions in Ukraine due to the COVID-19 pandemic disproportionately impacted the elderly, the poor, and families with children.

REGULATION OF PRIVATE BUSINESSES

The government has taken steps to scale back regulation of private businesses in recent years. However, the business environment is negatively affected by widespread corruption, and a moratorium on the sale of agricultural land remains in effect until July 2021.

The COVID-19 lockdown was not enforced equally for all businesses in Ukraine. Some businesses that belong to politically connected individuals were allowed to operate with few restrictions, while other nonessential businesses were forced to close down.

SOCIAL FREEDOMS

The government generally does not restrict social freedoms, though same-sex marriages are not recognized in Ukraine. Domestic violence is widespread, and police responses to the few victims who report such abuse are inadequate.

TRAFFICKING OF WOMEN

The trafficking of women domestically and abroad for the purpose of prostitution continues. IDPs are especially vulnerable to exploitation for sex trafficking and forced labor.

MINIMUM WAGE

Labor laws establish a minimum wage that meets the poverty level, as well as a 40-hour work week and workplace safety standards. However, workers at times go unpaid, and penalties for workplace safety violations are lenient.

•Anisha Agarwal*, Sanctity of Personal Data: A Comparative Study of Data Privacy Laws in EU, US and India,* International Journal of Legal Developments and Allied Issues/The Law Brigade, Vol. 6, Issue 3, May 2020. This is an in-depth analysis by Anisha Agarwal of the existing Data Protection Laws in the United States, the EU and India. The ground level of data protection law was established with implementation of the Lisbon Treaty of 2009. This was followed by the Article 95 Treaty which set forth the general harmonization clause as the foundation stone of the EC secondary data protection law. Directive 95/46/EC served the dual purpose of unrestricted movement of personal data and individual data protection rights. The complete circle of regulatory acts was completed by Directive 2002/58/EC on privacy and electronic communications and Regulation 45/2001/EC on data protection rules for artificial persons. The Framework Decision 2008/977/JHA was adopted in 2008 to lay all-embracing data rules for the EU. In 2016, the EU replaced the Data Protection Directive with the GDPR after four years of negotiations and "umpteenth amendments," bringing an end to the mutilated data practices across the EU which had caused legal uncertainties among the member states. With the resulting constant safeguards throughout the EU, the prospective barrier for the free movement of data have been eliminated to a great extent.

Agarwal also provides a useful comparison between the EU and the US approach towards data protection, with striking similarities and differences based on the different approaches towards data protection legislation by each. In the context of supervision, the EU and the US have each discussed and "imbibed" the concept of supervision and oversight, but there is still a slight point of difference in their definition, where the EU believes in supervision independent of the nature of the agencies whereas the US is inclined towards the internal supervisory mechanism.

•Sven Daniel Wolfe, *Between the Minor and the Intimate: Encountering the Authoritarian (extra)ordinary in Russia, Belarus and Ukraine*, Geopolitics 2021. Authoritarianism has been a favorite topic for scholarship in post-Soviet countries since the fall of the USSR. This article by Sven Wolfe addresses an alternative way to assess intimate geopolitics and analyze geopolitical complexities, from the intimate perspective of the domestic individual, in this case an American who has lived in Russia before, during and after Vladimir Putin was Prime Minister and then President. The observations throughout this narrative are written from a feminist geopolitical perspective, and are personal in their description of the collisions between authoritarian practices and individual lives during such mundane and everyday events as arriving at an airport, checking into a hotel, going for a hike, and witnessing the practical challenges of living and working in conditions of increasing authoritarianism and gathering meaningful information in contexts dominated by authoritarianism and illiberal practices. The micropolitics and micropolitics are mutually constitutive, and neither can be understood without the other. The author concludes by noting that there is an alarming intensification of

authoritarian practices in Russia and Belarus, and that both countries are experiencing an intensification of illiberal practices of late, such as stolen elections, police crackdowns, destruction of independent media and mass arrests. In contract. The policy in Ukraine has moved toward democratic representation, government accountability, support for independent media, and something of a haven for Russian speakers escaping from Russia or Belarus.

V. LAW OF UKRAINE ON PROTECTION OF PERSONAL DATA

Effectiveness of Draft Laws of Ukraine on Protection of Personal Data:

•*Law of Ukraine on Protection of Personal Data.* This is the full text of the Law of Ukraine on Protection of Personal Data in force since January 1, 2011. The Law provides that any individuals concerned must give their consent to the processing of their personal data (except for anonymised data), where such data is deemed to be restricted-access information.

THE CONSENT REQUIREMENT

An important definition of consent to data processing was reintroduced to the Law at the end of May 2014 after having been formerly removed for some time. Consent is now defined as *the voluntary, informed permission of individuals with respect to the processing of their personal data according to the defined purpose of processing.* This permission must be expressed in writing or in a form which enables verification that such consent was actually provided. With respect to minors, consent should be provided by one of their parents or by a guardian (as applicable).

Notification of the processing of certain personal data about individuals is usually not sufficient; the data controller must generally obtain explicit consent. There is no specific requirement for a strict 'working' consent form. However, the Ombudsman has released an indicative consent form, which seems to be appropriate only for written consent (it appears to have requirements which are excessive or unnecessary for electronic consent). In any event, a business is free to use its own corporate templates for consent, provided that they comply with the requirements of the Law. When giving their consent to the processing of personal data, data subjects are entitled to limit the scope of the data processing activity undertaken by the database owner.

In the e-commerce sphere, a data subject's consent may be provided during their registration in the respective communication system of the e-commerce subject, by way of ticking the 'consent box' in the system, and only provided that such a system does not allow the processing of personal data before the box was ticked by a data subject.

Furthermore, the Law establishes certain cases when consent is not required, specifically:

- when it is explicitly provided for by law; and
- where the data is necessary for the purposes of maintaining national security, economic welfare, and for the protection of human rights.
-

OPENNESS AND TRANSPARENCY

Openness and transparency: Processing of personal data should be conducted openly and transparently with use of means and in a manner which meets the purposes of such data processing.

Accuracy: Personal data must be precise and accurate and be updated to the extent needed.

Data minimisation: The content and the volume of personal data must be relevant to, adequate, and not excessive as regards the defined purpose of processing

DATA TRANSFERS

The Law requires that personal data can only be transferred to countries which provide an adequate level of data protection. Specifically, the Law outlines that the members of the European Economic Area ('EEA'), as well as all other countries who joined Convention 108, would be considered to provide an adequate level.

The above list is not exhaustive, and the Law provides that other countries that provide an adequate level of data protection (i.e. non-EEA members and non-members of Convention 108) will be defined separately by the Cabinet of Ministers. This is of central importance in terms of business activity in Ukraine, where business relations have been developed with, *inter alia*, the USA and Canada, despite both of these countries being outside the EEA and Convention 108. Until now, no such list has been developed and adopted by the Cabinet of Ministers.

LEGAL JUSTIFICATION FOR CROSS-BORDER DATA TRANSFERS

The Law offers five alternative grounds which may serve as a legal justification for cross border data transfer and provide business entities some room to process personal data internationally.

These grounds are:

- the provision of unambiguous consent by the data subject;
- the necessity to conclude or fulfil an agreement between the data controller and a third party for the benefit of the data subject;
- the necessity to protect vital interests of the data subject;
- the necessity to protect public interest or pursue legal remedies; and
- the provision for relevant guarantees by the data controller regarding the non-interference with the private and family life of the data subject.

THIRD PARTY ACCESS TO PERSONAL DATA

According to the Law, third party access to personal data should be governed by the terms and conditions of the data subjects' consent to the processing of their personal data. If the consent provided by the data subjects covers the possibility of the database owner to provide access to third parties, then the provision of such access will be permitted.

Further to this, the Law explicitly states that a third party may not be granted access to certain personal data if it refuses, or is unable to commit to, or is unable to fulfil the provisions of the Law (including those regarding the protection of personal data).

In order to access personal data, third parties must make an official request to the database owner. The request must contain information relating to:

- the full name and contact details of the third party;
- the name and other details of the individual whose personal data is requested which enables the owner to identify the individual;
- the database from which the request is being made, or the owner/manager of the database;
- the list of personal data requested; and
- the purpose and/or legal grounds of the request.

Third party access to personal data may be chargeable, by an amount to be decided by the Government of Ukraine ('the Government') for the state authorities, and, in the private sector, by companies themselves. However, unlike third parties, individuals have the right to free access to their personal data stored in a database.

DATA RETENTION

According to the Law, personal data must be destroyed or removed in the following cases:

- the expiry of the time frame of the storage of data, specified if the data subject's consent agreement for the processing of said data or by law (in certain cases the law defines the term of storage of specific data, which cannot be amended (shortened) by the consent);
- the termination of legal relations between the data subject and the data controller or data processor, unless otherwise provided by law; and/or

- the effect of a court decision on the removal of the data of an individual from a personal database.

Additionally, personal data must be destroyed or removed in other circumstances prescribed by law.

Retention of personal data implies actions aimed at the preservation of the established regime of access to such data.

The retention term shall be provided in the data subject's consent or by law. Upon expiration of such term the personal data shall be destroyed.

CHILDREN'S DATA

There is no separate provision in the Law which would touch upon the regulation of processing children's data. Therefore, in this context general rules apply, i.e., that parents or guardians should provide consent to processing of children's data, unless otherwise provided by law. This does not relate to the legitimacy of the processing and some exceptions may apply. Under the general rule, children are persons under the age of 18. In some cases, provided by law children may generally enter into contracts from the age of 16, which implies that they can provide consent to processing of their data with the specifically defined purpose (related to entering into respective contracts) before they reach 18 years old.

SPECIAL CATEGORIES OF PERSONAL DATA

Sensitive data

Notably, the processing of sensitive personal data is explicitly prohibited.

The Law further provides for a range of exemptions from the rule relating to the processing of sensitive personal data. In particular, this restriction does not apply to cases where the processing of personal data concerns, *inter alia*:

- sentences in criminal cases;
- the provision of some medical services by medical practitioners bound by professional non-disclosure obligations; and
- personal data which was made publicly available by the data subject.

Special risk data

The Law also includes a definition of another type of data: 'data which comprises a special risk for the rights and freedoms of individuals' ('Special Risk Data'). In turn, the Ombudsman has established a list of the types of Special Risk Data (Article 1.2 of the procedure for notification about the processing of personal data which is of a particular risk (only available in Ukrainian here), which is not entirely the same as sensitive data. Specifically, in addition to sensitive data, the following are recognised as Special Risk Data:

- nationality;
- an individual's location and routes of movement; and
- information as to whether an individual has suffered from violence or other abuse.

The Law provides for a slightly different regime for Special Risk Data. In particular, a data controller must notify the fact of processing Special Risk Data to the Ombudsman. This is a post-factum notification, which should be made within 30 days of beginning the processing of Special Risk Data. The notification is subject to a formal procedure adopted by the Ombudsman. At

the same time, some exemptions apply (e.g. processing of certain Special Risk Data for employment purposes).

DATA SUBJECT RIGHTS

Under the Law, data subjects have several rights relating to their data, including:

- to know the location of the personal database containing their personal data;
- to obtain information about the access of third parties to their personal data;
- to access their personal data;
- to obtain the contents of their stored personal data;
- to object to the processing of their personal data by the data controller;
- to request the modification or the deletion of their personal data by any data controller or data processor;
- to withdraw their consent to the processing of their personal data; and
- to be protected against automated decisions which have legal implications for them.

THE LIABILITY LAW AMENDING THE CPC

In June 2011 the Parliament adopted the Law of 2 June 2011 No. 3454-VI on Amendments to Certain Legislative Acts of Ukraine Concerning the Strengthening of Responsibility for Violation of Legislation on Personal Data (only available in Ukrainian here) ('the Liability Law'), which

strengthens administrative and criminal liability for failure to comply with data protection laws. The Liability Law amends the Criminal Code of 5 April 2001 No. 2341-III (only available in Ukrainian here), the Code of Administrative Offences of 7 December 1984 No. 8073-X (only available in Ukrainian here), the Criminal Procedure Code of 12 December 1960 (only available in Ukrainian here), and the Law of Ukraine of 2 October 1992 No. 2657-XII 'On Information' (only available in Ukrainian here), to establish individual responsibility for violations of legislation on personal data protection. Before the enactment of this law, the regulation of such liability was vague, and the strength of the sanctions which could be imposed was too weak to be a deterrent for any infringers.

The Liability Law has been fully effective since mid-2012 and has been further altered by the Amendments, with came into effect from 1 January 2014.

ADMINISTRATIVE LIABILITY FOR INFRINGEMENTS

Although the Amendments narrowed the administrative liability for infringements in the data protection area (mostly due to the abolition of the obligation on data controllers to register personal databases), some sanctions for non-compliance with certain data protection rules still exist. For example, failure to inform the Ombudsman of processing of eligible personal data may result in a fine in an amount of up to UAH 34,000 (approx. €1,100). Furthermore, illegal collection, storage, or dissemination of personal data could even lead to criminal liability, including the imposition of large fines, or even imprisonment for a term of up to five years.

•Yaropolk Brynykh, Head of Digital Rights GS of the NGO Digital Security Lab, *Internet Freedom Report 2020: Respect for Human Rights and Fundamental Freedoms on the Internet*, ABA Rule of Law Initiative in Ukraine.

The Internet Freedom Report 2020 is a bold and encouraging narrative that begins and ends on a high note. Opening with a discussion of the favorable environment for the Internet Freedom, it covers in extraordinary detail protection against cybercrime, digital literacy and freedom of expression, then turns to freedom of thought, the right to receive and impart information, freedom of online media, and legality and the need for legitimate restrictions in a democratic society. It then addresses freedom of peaceful assembly and association, freedom to use online platforms, and restrictions on freedom of assembly and association on the internet. Finally, its focuses on the right to respect for private and family life, protection of personal data and surveillance, and respect for human rights in the activities of internet intermediaries.

KEY POINTS IN THE PROLOGUE

The world and Ukrainian trend today is full digitization. With the Internet access and devices whereby one can benefit the World Wide Web services becoming more affordable, online threats have increased.

EFFORTS TO ELIMINATE ONLINE THREATS

Where there are threats to civilians, the State very often and very quickly emerges and seeks to eliminate those threats. However, very often such attempts end up in their opposite and result in the violation of digital rights.

ROLE OF INTERNET INTERMEDIARIES AND THE STATE

The Internet, as an environment for the realization of human rights, is also unclassified: in addition to the relationship between the State and the user, the role of such actors as Internet intermediaries is important. They may also violate human rights in their activities by unlawfully transmitting personal data to third parties, blocking users' access to websites, or not removing content containing a language of hostility. However, they are often beyond the reach of the State, because they are not under its jurisdiction.

THE STATE OF REGULATION OF THE TRIANGLE SYSTEM

This report initiates a tradition to hold an annual complex analysis of the state of regulation of the triangle system "State – User – Internet Intermediary" in Ukraine. In doing so, it provides a logical and clear outline of the current regulation of legal relations arising from Internet use in Ukrainian, a starting point for further research, as well as a basis for describing the main trends of such regulation during 2020.

DRAFT LEGISLATIVE AND GOVERNMENTAL INITIATIVES

The Report analyzes draft legislative and governmental initiatives published during the year, adopted acts as well as case laws, and formulates recommendations to the responsible authorities, with the hope of implementing at least some of them in 2021. The analysis concludes on an encouraging note.

•*Ukraine: Violations of User Rights*, Freedom House 2020. This report should be read in tandem with *Ukraine: Partly Free*, Freedom House 62/100, the Freedom House annual report on Ukraine. The COVID-19 pandemic saw the authorities prosecute users for spreading rumors online and launch initiatives aimed at stopping the spread of the coronavirus disease. This included an app that monitors individuals in mandatory isolation and infringe upon users' privacy rights. Online journalists continued to face extralegal retaliation for their work, and cyberattacks remain a regular occurrence, affecting government and nongovernmental targets alike.

•Aristova I. V, Tkachenko V.V., *Interaction of the Rules on Information Law of Ukraine and International Information Law: Development Trend.* The orderly and coherent formation and adoption of Ukrainian information legislation requires substantial coordination and joining of efforts of public authorities, civil society institutions, and the domestic scientific community as they collectively undertake the task of developing special rules and regulations that can be adapted to international legal standards as a key part of development of an information society. Ukrainian information legislation and its ultimate integration into the EU requires a carefully calibrated adaptation of that legislation to the international legal standards in effect only since the end of the 20th Century and the beginning of the 21st Century. For Ukraine, this effort calls for visionary and flexible thinking, a systematic social development process, a coherent process that leads to Ukraine's integration into a global information society.

OECD September 25, 2020, *Access to Justice and the COVID-19 Pandemic: Compendium of Country Practices*, accessible at https://www.oecd.org/governance/global-roundtables-access-to-justice/access-to-justice-compendium-of-country-practices.pdf

Ukrainian Access to Justice School of Practice programmes in response to COVID-19

The Ukrainian Access to Justice School of Practice is an educational platform co-founded by the Ministry of Justice, Legal Aid Ukraine, Association of Legal Clinics of Ukraine, Legal Development Network, and Ukrainian Legal Aid Foundation. The School has now adjusted its work to the current crisis. Several programmes of the School took action, in particular:

1) **To address the vulnerability of marginalized groups during the pandemic**, one of the School Programs -- Laboratory of initiatives to strengthen A2J for groups vulnerable to HIV -- started to research the pandemic-related legal issues of groups vulnerable to HIV.

Of the 75 surveyed respondents, 61% said to be facing pandemic-related legal problems, which included difficulties to access the health system. Based on the results, the Program developed both an immediate and longer term strategy of action, which is planned to include: - a course and practical guidance for lawyers on 'How to protect people vulnerable to HIV (based on the most urgent problems)'; - trainings for Legal Aid Ukraine centres' specialists on protecting the right to medical care for people vulnerable to HIV and take action against discrimination; - advocacy efforts, as well as the creation of educational videos/leaflets to share in social media; and -

development of guidelines on how to access legal aid guaranteed by the law through online tools.

2) The second Program, **Pro Bono Lab**, was transformed to help NGOs in the crisis. At the beginning of lockdown measures, a survey was conducted on NGO legal needs. The identified problems mostly concerned tax, rent issues, problems with online management, setting up the remote work with clients, security in the web. In line with the results, the Program developed webinars and short videos to be posted in social media and help NGOs cope with the crisis.

3) **Legal IT HUB** usually works on innovative technological solutions in the area of access to justice and community management. Faced with the quick transition of a large part of legal and social life to the web (and related problems, such as cyberbullying, new forms of discrimination, cybercrime, etc.), the Program team worked on the urgent response to these challenges by sharing practical tips for remote work, and overviews of remote management tools, overviews on cybersecurity and overviews of online training tools.

4) **The Legal empowerment of communities** Program and the Paralegal educational Program, which train community activists to conduct research on legal needs in their communities, switched to online trainings.

•*Justice Under the COVID-19 Pandemic,* Access to Justice in Eastern Europe, Issue 2/3(7), 2020. The 2020 COVID-19 pandemic has touched all mankind. Our health is put at risk and our everyday lives have been transformed. Many social institutions no longer function effectively in the new reality of the measures governments have taken and the lockdowns

ordered in an attempt to halt or at least mitigate the danger. The efforts of authorities and researchers all over the world are directed at the creation of approaches to deal with the new reality and the issues it raises. These efforts include the development of special adaptive regimes that will ensure the possibility of effectively performing everyday social functions now and, if needed, in the future. Access to justice is an integral element of a rule-of-law democratic state, a common value of human civilization, the effective implementation of which symbolizes the high level of our social evolution. In the context of the rapid spread of the coronavirus, the hospitalizations and lockdowns, the public health measures such as mask-wearing and social distancing, the duty to administer justice properly and in a timely manner has become a difficult task. The general lack of preparedness by legislative and judicial institutions beforehand, and the seemingly ad hoc approaches and development of actions in response to the pandemic have led to outcomes the meaning and consequences of which we will be contemplating and evaluating for a long time. This special double issue of our journal is symbolic. The arrival of COVID-19 in the early months of this year has had an impact on all spheres of our lives, including scientific and publishing activities. The disruption of plans and schedules, and, most importantly, the changes in our perceptions and feelings about the reality around us which the pandemic has brought with it, have affected us directly, too. The preparation of a special issue devoted to access to justice in Eastern Europe amid the challenges brought about by the pandemic is an attempt to attract attention and intensify research in this subject area.

THE UKRAINIAN EXPERIENCE OF JUSTICE UNDER COVID-19

The Ukrainian experience of justice under COVID-19 is presented in four articles, with the general focus on the organization and functioning of the judiciary, and special attention to its financing, as well as peculiarities in relation to consideration of civil and criminal matters. The first of these by Serhii Prilutskyi and Olga Strieltsova describes the main challenges that the Ukrainian judiciary faces this century and especially those amid the pandemic. The state of affairs seems to be the logical consequence of deeply systemic problems that have accompanied the evolution of the judiciary in Ukraine since it became an independent state, at that time and still today significantly influenced by both the post-Soviet legal heritage and the complex of contemporary challenges the Ukrainian judiciary faces – from the onset of military actions in the east of Ukraine to the COVID-19 outbreak. The pandemic shows how vulnerable the judiciary is. One path forward is to find a new vision and a new understanding of the judiciary in order to ensure its normal functioning, as well as to ensure accessible and effective justice, perhaps partly through lessons learned in the experience with the pandemic. One of the most difficult steps taken in Ukraine during the pandemic has been the provision of normal funding for the work of government agencies, including the judiciary.

Tetiana Korotenko and Iryna Kondratova provide a study of existing approaches to the financing of the judiciary in Ukraine is undertaken, in particular an assessment is made of the measure as a result of which the salary of judges was reduced during the lockdown. Using the example of a complex court case which passed all judicial instances in the state as well as

studies of the main approaches that were implemented in independent Ukraine, the authors offer conclusions about the possibility of the financial autonomy of the judiciary. Traditionally in Ukraine, procedural timeframes have been established by law or decided by judges with the aim of having a fair and timely trial and establishing equal access to justice for both parties. Today, new legislative COVID-19 regulations break with this approach and create a new vision of trial timeframes.

Oleh Rozhnov explores the determination of timeliness in the consideration and resolution of civil cases under the conditions of a lockdown in response to the pandemic. In particular, the author criticizes the adoption by the legislator of measures for the automatic extension of procedural deadlines as those that violate the basic principles of civil proceedings and the right of a person to a quick and fair trial.

The most important issues of access to justice and fundamental rights in criminal matters are offered by Oksana Kaplina and Svitlana Sharenko. Some significant remarks are made in their study concerning the derogation of the European Convention and the various measures intended to help maneuver through, as well as successfully deal with the main challenges to the judiciary in matters of criminal law under the conditions of the COVID-19 pandemic in Ukraine.

•Elyssa Shea & Marta Jaroszewicz, *Opening in Times of Crisis? Examining NATO and the EU's Support to Security Sector Reform in Post-Maidan Ukraine,* East European Politics 37:1, 2021. Security sector reform has

remained largely disconnected from the broader debate on societal transition in the literature thus far. This article analyzes how external support to security sector reform could potentially facilitate socio-political order opening in a limited access order. Based on two dimensions, the authors examine the case of NATO and EU's support to Ukraine's security sector reform between 2014 and 2019. NATO's support to the military and the EU's support to the police and state security service (SBU) appear unlikely to cause opening of the social order, while NATO's support to the military-industrial complex is more likely to cause opening.

In the wake of Ukraine's “Revolution of Dignity”, which began in 2013 and continued into 2014, and during an ongoing conflict in Eastern Ukraine, the Ukrainian government requested assistance for its SSR process. Based on theoretical conceptualization of how opening could be promoted by external actors, we examine the case of the EU and NATO's support to SSR in Ukraine. The authors theorize that NATO's support to the military as well as the EU's support to the police and state security service (SBU) look unlikely to cause opening of the social order, while NATO's support to the military-industrial complex is more likely to cause opening.
The authors begin with a literature review on SSR, noting evident gaps in the literature, then outline further concepts from the literature on SSR and Europeanisation beyond the EU, putting forth two dimensions for evaluating whether support to SSR could promote opening. In their empirical case study, the authors introduce the dynamics of Ukraine as a limited access order. They then analyze NATO and the EU's support to SSR

in light of our dimensions for facilitating opening, before making concluding remarks.

UKRAINE AS A LIMITED ACCESS ORDER

Ukraine could be classified as a LAO, a Limited Access Order, with relatively high political and economic access as compared to other countries in the region, leaving some room for "domestic hooks" that external actors could use to promote opening (Ademmer, Langbein, and Börzel 2019, 205). Relative to other LAOs in the region, it is one of the most likely cases for opening (ibid.; Vilpišauskas et al. in this volume). Yet, despite repeated political upheavals and formal changes of the government in the last decades, Ukrainian political and economic elites have largely replicated a model of oligarchic governance (Kostiuchenko and Melnykovska 2019). Transition to an OAO in this case would require targeted and extensive effort on behalf of external actors, as the LAO is otherwise likely to remain stable (Ademmer, Langbein, and Börzel 2019, 205). Ukraine's security sector in particular is known to offer a major source of rent-seeking for elites in terms of potential political power and ability to collect economic resources (Ivashchenko-Stadnik et al. 2018). Hence, reform to Ukraine's security sector could be a key aspect of its transition to an OAO.

THE CONTEXT OF UKRAINE'S REVOLUTION OF DIGNITY

In Ukraine, the government's decision to increase SSR efforts in 2014[6] was prompted by the reaction to brutal suppression during the "Revolution of Dignity" protests and the outbreak of the conflict in eastern Ukraine. After President Viktor Yanukovych's decision to end talks on a Ukraine-EU

Association Agreement in November 2013, pro-European Ukrainians demonstrated for months on Kyiv's Maidan square. These protests were largely against the corruption of President Yanukovych's regime (Fluri and Badrack 2016). Berkut forces, an elite riot police run by the Ministry of Interior, violently tried to disperse the demonstrators on multiple occasions, resulting in over a hundred fatalities and around a thousand injuries (ibid.; *BBC* April 4, 2014).

UKRAINE'S POWER VACUUM IN 2014

In the power vacuum that occurred after President Yanukovych fled the country in February 2014, Russia annexed Crimea in March 2014. Pro-Russian separatists then made several bids to overthrow local government institutions in eastern Ukraine, resulting in the ongoing conflict between these forces and the Ukrainian armed forces. The Ukrainian security institutions that existed in March 2014 "were unable to respond effectively to the emerging conflict in Eastern Ukraine" (Oliker et al. 2016, xiv) and also fell short in terms of legitimate use of force during the Revolution of Dignity (Litra, Medynskyi, and Zarembo 2017, 28). This context prompted Ukraine to launch a comprehensive review of its security sector and to ask for increased foreign assistance.

NATO'S APPROACH: PARTNERSHIP FOR PEACE

Ukraine was the first post-Soviet country to join NATO's Partnership for Peace programme in 1994. During the time in which Ukraine was officially non-aligned, cooperation remained primarily on the level of professional trainings for the military. This changed after the conflict in Eastern Ukraine broke out in 2014. In 2017, Ukraine's law on foreign policy officially

declared desire for Euro-Atlantic integration, and in 2019, the *Verkhovna Rada*, Ukraine's parliament, officially backed amending the constitution to explicitly state Ukraine's path towards NATO and the EU (*Unian,* February 7, 2019).

Since 2014, NATO has increased its presence in Ukraine. The NATO Representation to Ukraine now encompasses both the NATO Liaison Office and the NATO Information and Documentation Centre. The former is part of the Political Affairs and Security Policy division of NATO, while the latter is engaged in strategic communication towards Ukrainian elites and public and facilitates stakeholder meetings. At the onset of its increased assistance in 2014, NATO primarily focused on the armed forces and Ministry of Defence. In 2016, it increased its engagement to the security sector more broadly, providing support to the National Guard, Border Guard Service, parliament, the Ministry of Interior, State Security Service of Ukraine, and civil society.

THE EU'S APPROACH SINCE 1994

Ukraine's relationship with the EU was formalised with a Partnership and Cooperation Agreement in 1994 (EEAS 2019) and in 2009 it became part of the EU's Eastern Partnership programme. However, the EU only began to factor a clear security dimension into its approach to Ukraine after the events of 2014 (Litra, Medynskyi, and Zarembo 2017), despite the 2009 Eastern Partnership's declared aims of delivering security and prosperity to the country (European Commission 2009). The 2015 European Neighbourhood Policy review proposed stronger security cooperation, portraying the EU's Common Security and Defence Policy (CSDP) missions

to Ukraine as an important part of this (European Commission 2017a). While the EU has emphasised the importance of both civilian and military capabilities in its strategic documents about SSR support (European Commission 2016), all assistance provided to Ukraine has been civilian. The EU's support to SSR in Ukraine has primarily occurred through the European Union Advisory Mission in Ukraine (EUAM), which launched in 2014 and is under the CSDP. These efforts should complement the EU's wider state-building support to other sectors through the Association Agreement and Support Group for Ukraine. EUAM has been engaged in assistance to the Ministry of Interior, National Police, SBU, State Border Guard Service, General Prosecutor's Office, local courts, the parliament and civil society (EUAM 2020).

EMPIRICAL ANALYSIS

The following sections analyze NATO and the EU's support to SSR in light of the dimensions that we conceptualize as relevant to social order opening. Looking at the SSR support the EU and NATO have provided, we selected four areas receiving support. Based on an empirical analysis of these four areas using our theoretical dimensions, we present the least through most likely areas where external support to SSR may cause opening in Ukraine's LAO: the military, the police, the SBU, and the military-industrial complex (Table 2).

In the context of Ukraine, it should first be noted that the military itself has not had a pivotal role in perpetuating the nature of the LAO. Even in Soviet times, the military was largely not “politically ambitious” and was subject to “policy, rather than the master”, operating with a fair degree of

professionalism (Sherr 2001, 1). In Ukraine, the internal security agencies have been more problematic in terms of their lack of political control under clearly defined rules (ibid., 3). Informal control of the internal security agencies as one of multiple centers of power has been one way of stabilizing the LAO.NATO has been the main external actor in support to reforming Ukraine's military. The core over-arching goals of NATO's assistance has been to "strengthen democratic and civilian control of Ukraine's armed forces and security institutions" (NATO 2019a) and boost Ukraine's ability to provide for its own security (NATO 2019b). Its strategic-level advice has been consolidated alongside technical assistance and capacity-building under NATO's Comprehensive Assistance Package (CAP) (NATO 2016).[15] Enacted in 2016, the CAP has aimed to support the objectives of Ukraine's Strategic Defence Bulletin, which was drafted with NATO assistance and states Ukraine's aspiration to reform its armed forces according to NATO standards and achieve interoperability with NATO forces by 2020. This also includes "trust funds" worth 14 million euro to help Ukraine upgrade its defence system.[16] These trust funds are voluntary, nationally-led and funded projects in vital areas such as C4 (Command, Control, Communications, and Computers). On a bilateral level but within the NATO framework, the United States (US), Canada, Poland, and Lithuania, have also provided training and military aid to the Ukrainian armed forces.[17]

A vast amount of overall support provided by NATO concerns security assistance to the conflict in Ukraine's east, rather than SSR targeting the criteria for transition. Given the relative lack of utility of the military to the

dominant coalition prior to 2014, military reform and funding were neglected during the presidency of Viktor Yanukovych from 2010 to 2014 (Melnyk and Sungurovsky 2013). Circa 2014, the armed forces were largely ill-equipped to effectively combat a military threat to the central Ukrainian government on the country's territory (Oliker et al. 2016). This has been a focal point of NATO's assistance due to its own security interest in preventing further escalation of the conflict or loss of further Ukrainian sovereign territory.

In terms of SSR support, NATO consulted heavily on the drafting of Ukraine's "Law on National Security", towards the aim of installing civilian control measures and defining the relationship and competences of Ukraine's security institutions within a legal framework. While Ukraine already established a parliamentary committee in the 1990s with the purview of overseeing the defense budget – the Committee for Security and Defense – in actuality it has not been performing this function effectively. The committee has often lacked expertise, faced resistance from the executive, and lacked access to detailed information regarding defence expenditures due to current over-classification (Bugriy and Maksak 2016). NATO advised that specification of the parliament's role in supervision be included in the new national security law (National Institute for Strategic Studies 2018). It also stipulated the need for a civilian defence minister by 1 January 2019.NATO's support has been invaluable in terms of supporting Ukraine's military as regards immediate threats to its national security, but this aspect has dominated its focus. Such superficial attempts at refining political control over the military look unlikely to cause opening

in light of the military's relatively weak role in the LAO and due to the lack of impersonal, specialized institutions, which would allow for more effective political control in practice. In this case, it looks unlikely that this aspect of NATO's SSR support will cause opening. It should be noted that part of NATO's engagement happened through the "international advisory group" to Ukraine. This informal advisory body consists of NATO, the US, and the EU (both the EU Delegation and EUAM), and has met *ad hoc*, at times on a daily basis. The group has focused on SSR, coordinating joint steps and its messaging to the Ukrainian government and public. The international advisory group consulted on the national security law and supported conditioning US military aid on its passage. The new national security law ultimately passed in 2018, including a clause on the need for a civilian defence minister but maintaining the hierarchy of the executive as dominant in supervision over the sector (Tregub 2018). NATO bilaterally and the advisory group have continued to call for the law's implementation and development of secondary legislature in political statements (NATO 2019b)

In light of NATO's assistance to the military being primarily focused on security assistance and rather modestly playing a role in facilitating political control over security in the LAO, it is unlikely to cause opening. Nevertheless, there have been multiple incentives present in this area that still make elites prone to accept assistance, even if this merely promotes the status quo. Post-2014, NATO supported Ukraine's membership aspirations, though this was not yet what would be considered official support to NATO accession.[23] While Ukraine has not been granted a Membership Action Plan,

the Annual National Programs of Ukraine-NATO cooperation have specifically emphasized democratic reforms and "performance" is concretely assessed by allies on a yearly basis. In June 2020, NATO also granted Ukraine an "Enhanced Opportunities Partner", a further signal of deeper partnership (NATO 2020). Alignment with NATO has become increasingly attractive to the Ukrainian elite since 2014 in light of the perceived security guarantee it brings (Samokhvalov 2015).

Furthermore, NATO has linked its reform agendas on civilian control on a declaratory level and in its advisory capacity when drafting new strategic documents to its military aid. As noted, conditionality was used regarding US military aid through international advisory group to ensure passage of the new national security law, although the law ultimately did not fully comply with all NATO recommendations. Security assistance from NATO member states has been perceived as key to reform of the Ukrainian armed forces' training system, which was particularly important in the first stage of the conflict, and it has therefore been in the interest of elites go ahead with some reform linked to this. Ukrainian elites claim that military institutions and instruments should be the primary focus in light of the imminent threat posed by war in the east. There has been some questioning on the Ukrainian side of whether civilian control measures should really be a priority during a time of war. In this regard, security interests also seem to predominate for the external actors, as military aid has been provided despite a lack of full compliance with NATO reform demands.

In this article, we theorized how external support to security sector reform could promote transition from a limited to an open access order. Building on North, Wallis, and Weingast's (2009) logics of socio-political order transition, we conceptualized two dimensions for analyzing how SSR support might promote opening. First, it would need to target support to specific criteria in order to transition: political control over agents of force, impersonal, specialized institutions, and rules governing the use of force. Second, there would need to be incentives for elites to accept support that does target the criteria, taking into consideration the logic of the LAO. Depending on whether the support from external actors targets the necessary criteria and whether incentives are present, support may be more or less likely to cause opening. Deploying this framework, we analyzed NATO and the EU's SSR assistance to post-Maidan Ukraine, particularly concentrating on four areas: the military, the police, SBU, and military-industrial complex. We asked, to what extent do external SSR policies appear to have the potential to cause opening?

In looking at the SSR support that NATO provided to Ukraine, we conceptualized its support to the military as not very likely to cause opening, while its support to the military-industrial complex was likely to cause opening. Incentives have been present for the dominant coalition in both areas of support targeted by NATO, which we theorize as an important aspect of making it SSR support more likely to be accepted. US military assistance through the NATO framework has been particularly linked to progress in both areas of reform, such as the new law on national security in 2018 and "On the State Defense Order" in 2020.

NATO's support to the military largely dealt with security assistance in light of the war and rather shallowly dealt with political control, bringing about reform but not making it likely to cause opening. Its support to the military-industrial complex, however, comprehensively targeted the creation of specialized, impersonal institutions via reform to defense procurement and efforts at a more transparent system of classification for security-related data. Based on our empirical analysis of Ukraine, it looks unlikely that political control over the military will be effective until specialized, impersonal institutions are more fully in place in the military-industrial complex. In this regard, the need for an impersonal system for classification of sensitive information is urgent.

The EU's support to reform of both the SBU and the police has been largely devoid of incentives. The lack of concrete economic or security incentives attached to the EU's SSR support, particularly as compared to the military aid linked to NATO's support, provides little reason for the dominant coalition to opt out of their current system of rent-seeking. In the context of Ukraine's LAO, both the police and the SBU have played a major role in perpetuating the order and are thus likely to be particularly resistant to change. Thus, even though the EU has targeted support to impersonal, specialized institutions and rules through advisory and capacity-building efforts towards the SBU and the police, its support looks unlikely to cause opening. EU support to police reform advanced further than we would have expected and may have had some tangible security benefits for citizens, but has already shown signs of reversal.

Overall, in the unique context of Ukraine's wide-ranging reform efforts while at war, the security imperative and heightened geopolitical tension surrounding the conflict appear to have re-invigorated the attractiveness of closer cooperation with NATO and military aid in particular. The role of the US remains critical here. The EU has been less able to link its support to tangible incentives and continues to be perceived as an economic rather than security actor by the dominant coalition, which we conceptualize as harming its ability to deliver SSR support that might cause opening. There is some evidence of security interests on the part of external actors as well, given that conditionality attached to economic or military aid has not been fully applied or is not applied at all in some areas, even when reform does not occur or does not comply fully with Euro-Atlantic standards. It is clear that there is an interest in delivering military aid to Ukraine, considering that many EU and NATO member states neighbor the country and are seeking to avoid the conflict from spilling over. In any case, the international advisory group has provided a format for coordinating reform efforts, as evidenced by the joint support given by the US, EU, and NATO to the drafting of the national security law in 2018, and could be a useful channel in the future.

The empirical analysis also shed some light on NWW's theory in a modern context. It is clear that the different types of security institutions can play different roles depending on the context of the LAO. For Ukraine, as is the case for many post-Soviet countries, the internal security system appears to have a very powerful role maintaining order in the LAO through their collection and distribution of rents. Aside from the alleged abundant

opportunities for rent-seeking in the military-industrial complex, the military itself does not appear to play a large role in perpetuating the LAO. Furthermore, sequencing appears important in terms of reform targeting the criteria. Impersonal institutions and rules, which have dominated most of the support to the SBU and police as well as the military-industrial complex, are particularly important to focus on ahead of political control, which has been the main focus of assistance to the military.

While there has been criticism from the Ukrainian elite towards external actors that wider transformation cannot be effectively pursued during a conflict, NWW emphasize that opening has often happened as an unintended effect of elites opting for select changes in terms of impersonal institutions. At present, NATO's support to reform of the military-industrial complex in Ukraine appears particularly likely to achieve this.

•Orysia Lutsevych, *How to Finish a Revolution: Civil Society and Democracy in Georgia, Moldova and Ukraine*, Chatham House, January 2013. Civil society in Ukraine would benefit from Western support that focuses on building up moderate forces. Prioritizing greater citizen participation in organizations, as well as social trust, tolerance, openness and self-expression can do this. The domination of public space by the state and political life is suffocating liberal democratic developments in these countries. In order to expand the public space, donors can facilitate debate among citizens, helping to strengthen public opinion that could influence the

state. This requires long-term donor commitment as it takes time for new behavior to take root. Donors often switch focus between priorities and instruments aimed at enabling active citizenship, such as access to information, participatory councils, rural community centers, neighborhood associations and public spending monitoring. They would do better to invest more long-term resources into just one or two priorities that could produce a tipping point in empowering civil society.

Instead of attempting to replicate the better-funded programs that the US government has been implementing for decades, the EU could try different approaches to revitalize civil society. These could include switching from a top-down approach, whereby local NGOs are forced to work with the government, to a bottom-up one that would include West European grassroots organizations in program design and decision-making. In order to strengthen the role of civil society in policymaking and promote a more favorable attitude among the Ukrainian Government and local authorities towards their citizens, donors need to improve awareness of European practices in citizen engagement and community organization. Western financing could also support training for local leaders in community organization and mobilization. Donors could also consider supporting nonconventional actors beyond existing NGOs, such as youth groups, students' associations and universities, grassroots citizens' initiative groups, intellectual circles, schools and religious organizations that pursue charitable and community goals.

They could link teams of activists, creating more national and international networks, and create projects to stimulate new patterns of social behavior and provide a clear vision of an alternative future. The belief that few NGO leaders alone can prevent democratic backsliding is a fallacy. Donors should enlarge support to new groups in addition to funding well-established NGOs. Donors also need to consider incorporating conditionality in their support for NGOs, based on criteria including connections with citizens. This could mean requiring co-funding for projects from membership fees, a certain number of open community meetings in public places, media outreach in the community, and a share of volunteer work as a community contribution. To reinvent democracy support there is a need to return to the fundamental principle of a participatory democratic society where people have more say and more power.

As Karl Popper pointed out in *Democracy may help 78 Key Findings: Public opinion in Ukraine*, International Foundation for Electoral Systems, July 2011, http://www.ifes.org/~/media/Files/Publications/Survey/2011/Public_Opinion_in_Ukraine_2011_Report.pdf. "Helping citizens in the post-Soviet space to cherish freedom and embrace their responsibilities in a democratic system of governance is crucial ' www.chathamhouse.org page 19. *How to Finish a Revolution:* Civil Society and Democracy in Georgia, Moldova and Ukraine to preserve freedom but it can never create it if the individual citizen does not care for it.' Helping citizens in the post-Soviet space to cherish freedom and embrace their responsibilities in a democratic system of governance is crucial. For it will be these citizens, despite the weaknesses of civil society today, who will decide the future path of

Ukraine. Although voting in elections is an essential element of the process, if the citizens of Ukraine want true democracy, transparency and personal freedom, they also need to engage in public debate and build social trust. What was started on the central squares of Kyif during the Orange revolution must continue in self-expression and participation in public and political life.

****

POSTSCRIPT: WHERE DOES UKRAINE GO FROM HERE?

Russia's Aggression Against Ukraine Is Backfiring: Putin's military moves are rallying Ukrainians and unifying NATO.

By Kori Schake, *The Atlantic,* accessible online at *https://www.theatlantic.com/international/archive/2021/12/russia-putin-ukraine-invasion/621140/* (DECEMBER 29, 2021)

Western intelligence agencies have warned that Russia is contemplating an invasion of Ukraine, perhaps involving some 175,000 troops. Vladimir Putin's government has already moved more than 100,000 troops along Ukraine's borders, including into Belarus. Russian officials have been making outrageously paranoid and false accusations. Russian Foreign Minister Sergei Lavrov, for example, recently blamed NATO for the return of the "nightmare scenario of military confrontation." Russian Defense Minister Sergei Shoigu said that the United States is smuggling "tanks with unidentified chemical components" into Ukraine's Donetsk. And Putin himself has been equally vituperative about NATO, threatening military moves unless it agrees to his terms. "They have pushed us to a line that we

can't cross," he said on Sunday. "They have taken it to the point where we simply must tell them: 'Stop!'"

Yet a recent report concludes that despite its massive deployment and threatening rhetoric, Russia is not planning to invade Ukraine. The report, produced by the Critical Threats Project of the American Enterprise Institute, where I serve as the director of foreign- and defense-policy studies, together with the Institute for the Study of War, finds that the political and economic costs of an actual invasion are too high for Russia to sustain. "Putin may be attempting a strategic misdirection that impales the West in a diplomatic process and military planning cycle that will keep it unprepared," the report argues. Rather than directly invade Ukraine again, Russia instead seeks to further destabilize the country in advance of its elections, station troops in Belarus, divide NATO, and precipitate Western concessions to de-escalate the crisis.

Even without an invasion of Ukraine, Russia's military moves pose serious threats to America's allies, including the Baltic states. Russia demands, as the price of even considering drawing down its military buildup, that NATO accept a different security framework for Europe, abandon any future NATO accessions, and forswear military cooperation with any non-NATO state. The CTP/ISW assessment of Russia's intentions is consistent with the country's preference for hybrid, or threshold, warfare: the fusion of disinformation and political, economic, and military actions designed to immobilize or weaken adversaries without triggering an effective response. The terms are faddish, as though the practice were a new addition to the

inventory of warfare. In fact, the simplistic definition of warfare after the Cold War as only military operations was novel, and that narrow conception has now evaporated along with American military dominance.
Strategic failures are almost always failures of imagination, as with the Trojans failing to wonder what might be inside that gigantic wooden horse. We are now scrambling to think as creatively as our adversaries. But the U.S. has a number of advantages: time, allies, transparency, and right. Even though Russia's military deployments have been rapid, the U.S. and its allies recognized them early enough to alert one another and agree on a response. The gathering storm of Russian revanchism since Putin came to power conditioned a quick reaction; defense spending by European NATO members has been rising since Russia's 2014 invasion of Ukraine. Bilateral consultations and NATO meetings produced a set of potential political and economic sanctions, especially Russia's ejection from the SWIFT financial network, that ought to give Putin and his businessmen pause. Turkey is providing drones to Ukraine, the U.S. sent military advisers and Javelin missiles, and Germany is reconsidering the Nord Stream 2 Pipeline. Democratic societies are slow to align but durable once committed, and the U.S. and its allies have had time to organize.

In an effort to de-escalate the crisis Putin created, the Biden administration has ruled out deploying American forces to defend Ukraine. Joe Biden evidently hoped to prevent a war by miscalculation—one side misinterpreting the other's actions, and violence spiraling into a nuclear apocalypse. And although textbook military strategy considers telling an adversary what you won't do self-defeating, in circumstances where the

asymmetry of interest is so pronounced, putting a ceiling on potential escalation will likely make America's policy more credible. In the immediate aftermath of U.S. capitulation in Afghanistan, it just isn't believable to claim that the Biden administration will "fight any battle and bear any burden" for the independence of a still-corrupt post-Soviet government. Biden consented to Russia's demand for discussions of a new European security framework. That consent was unquestionably a concession, giving some standing to Russian concerns, and it has worried frontline NATO allies who have long-standing (and justified) fears of abandonment. If we had refused to even discuss Russian concerns, however, it is difficult to imagine sustaining the solidarity of the Western alliance or American public support for the risks and sacrifices that any response to Russia attacking Ukraine might entail. And agreeing to discuss Russia's version of post–Cold War history or its demands for a sphere of influence that would consign countries to Russian dominion is not the same as accepting them.
Having the discussions take place in a NATO forum, as Russia has now agreed to do, allows the West to showcase its increased solidarity. Russia's threats have unified the alliance. The discussions will also contrast the U.S.'s preferred model of power, which emanates from our ability to persuade others to share the burdens of what we're trying to achieve, with the model pursued by Russian and China, which relies on threatening nations into submission.

The United States and its allies have the easier side of that argument. As Ronald Reagan said, "There is a profound moral difference between the use of force for liberation and the use of force for conquest." Russia may mobilize

some support among countries that feel threatened by governments held accountable by their citizens, but the U.S. has the moral and mathematical advantage of arguing against strong states imposing their will on those unable to protect themselves.

Not that Ukraine is truly incapable of protecting itself. One other thing that may be restraining a Russian invasion of Ukraine is the fact that, even in the Donbas, the mighty Russian military has not succeeded in subduing Ukrainian resistance. Quite the opposite: Russia has enhanced Ukrainian national identity. A Russian occupation would encounter the sort of insurgency that the Russian military proved incapable of subduing in Afghanistan and Chechnya, despite its brutality. Half a million Ukrainians have military experience; 24 percent of respondents in one recent poll said that they would resist Russian occupation "with a weapon in hand." Russia might succeed in taking Ukraine, but it is unlikely to hold it.

NATO countries might not fight for Ukraine, but they're likely to arm and train Ukrainians to fight for themselves. A Russian invasion would open the floodgates of Western support for Ukraine, and activate similar mobilizations of civilian society among NATO frontline states. Putin's threats have already convinced Germans that Nord Stream 2 is not just a business deal, but rather a means of geopolitical leverage. The EU can use its regulatory tools on Gazprom and other Russian businesses seeking access to Europe's markets more aggressively, to scrutinize their practices and enforce compliance with the law.

Transparency is a potentially devastating tool against authoritarians, because corruption is delegitimizing. The governments of free societies already face public scrutiny, which positions them well to demand the same of others. Russia's leaders are afraid of accountability for their wealth; the revelations of corruption in the Panama Papers appear to have led Putin to unleash cybervigilantes against the U.S.

Russia's past attempts to intimidate Ukraine into not choosing a westward path have backfired. Fifty-eight percent of Ukrainians now say that they would vote for NATO membership, and the nation has developed a greater sense of national identity and a more resilient society. Sweden and Finland are moving into closer alignment with NATO, as Russia illustrates the dangers of remaining outside the Western mutual-defense pact.

NATO has held united, refusing to accept that Russia gets a veto over either its membership or its actions. The United States, while averting military involvement, has crafted a credible set of penalties and garnered international support for them. Putin lacks the imagination to see that launching successful military operations is not the same as winning a war, a lesson the U.S. recently relearned in Afghanistan. That Russia is now repeating the very mistake the U.S. made, and is slowly recovering from, is an ironic twist.

Human Rights Watch World Report 2022: Ukraine - Events of 2021 provided this sobering account of the past year. The report is accessible online at https://www.hrw.org/world-report/2022/country-chapters/ukraine

The armed conflict in the Donbas region of eastern Ukraine continued to pose a grave threat to civilian safety and impede access to food, adequate housing, and schools. Covid-19 pandemic-related travel restrictions, introduced by Russia-backed armed groups and the government, blocked access to health care and pensions and worsened hardships for the already impoverished population of the conflict-affected Donbas.

Armed groups forcibly disappeared, tortured, and arbitrarily detained civilians and repeatedly denied some of them access to urgent medical care. A bill reforming Ukraine's notoriously abusive security service advanced in parliament despite human rights concerns.
Members of groups advocating hate and discrimination continued putting ethnic minorities, lesbian, gay, bisexual, and transgender (LGBT) people and rights activists at risk, subjecting them to physical attacks and hate speech.

ARMED CONFLICT

A spike in hostilities, despite the ceasefire, led to civilian casualties. According to United Nations human rights monitoring mission reports, in the first six months of 2021, 56 civilians were killed or injured by shelling, small arms weapons fire, mine-related incidents, and unmanned aerial vehicles (UAV) strikes.

Russia-backed armed groups in Donetska and Luhanska regions continued to torture, arbitrarily detain, and forcibly disappear civilians and to deny

them access to medical care. As of July, an estimated 300-400 conflict-related detainees were being held by these armed groups.
There were no reports of prolonged arbitrary detention by the Ukrainian authorities in 2021. The investigation into alleged grave abuses in unofficial detention facilities by Ukraine's secret services in 2016 remained open and has borne no results.

Excessive and arbitrary restrictions imposed by armed groups in Donestska and Luhanska regions continue to unduly burden civilians. The Ukrainian government ended most Covid-19-related restrictions in June. In welcome moves, in August the authorities temporarily suspended the requirement for pensioners residing in nongovernment- controlled areas to regularly confirm displaced person registration and in September, announced plans to introduce remote identity verification. If enacted, the latter step would help address discrimination against pensioners residing in nongovernment-controlled areas, in particular helping to eliminate barriers that pensioners who cannot travel due to limited mobility have faced accessing their pensions since 2014.
Lack of access to quality health care remained a key concern for conflict-affected parts of eastern Ukraine, where approximately 1.3 million people continued to face difficulties in accessing essential health services. Women have been disproportionately impacted, due in part to limited options for maternal and other sexual and reproductive healthcare in these regions, the poor quality of these services, and traditional gender roles that leave women with little time and few resources to prioritize and address their own health.

RULE OF LAW & ADMINISTRATION OF JUSTICE

In October 2020, the Constitutional Court of Ukraine stripped the national anti-corruption agency of its essential powers, effectively dismantling the system of publicly accessible asset declarations. The ruling was followed by President Zelensky's bill to terminate the Constitutional Court's powers. Zelensky withdrew the bill in January.

The trial of four defendants over the 2014 downing of Malaysia Airlines flight MH17 advanced to evidentiary hearings.

An October 2020 draft law meant to reform the Security Service of Ukraine progressed in parliament, despite granting the agency overly broad powers without sufficient human rights safeguards.

The criminal case involving the 2014 abduction and torture of two Maidan protestors, which resulted in the death of one of them progressed in April, with two men arrested and charged. Also in April, a district court sentenced a leader of the responsible group to nine years in prison. The group, known as "titushky" consisted of anti-Maidan activists recruited by law enforcement to attack protesters during Maidan protests. In December 2020, the State Bureau of Investigations indicted a Maidan activist on homicide charges in connection with the February 2014 arson of the Party of Regions office.

A January European Court of Human Rights decision found that the Ukrainian government committed multiple breaches of the European

Convention on Human Rights in the course of public order operations during the Maidan protests, including the right to life, the prohibition of torture, and the right to liberty and security.

In May, parliament adopted a long overdue law aligning Ukraine's national legislation with international law to allow for effective domestic prosecutions of grave international crimes, including those committed in Donbas and Crimea. At time of writing, because Zelensky has not signed the law, it has not gone into effect. Additional changes are likely to be needed to the Criminal Procedural Code to support effective investigations and prosecutions.

In late June, Ukraine's prosecutor general removed Gyunduz Mamedov as director of the government's specialized war crimes department. Human rights and watchdog groups criticized the decision as groundless and politically motivated.

FREEDOM OF EXPRESSION & ATTACKS ON JOURNALISTS

Physical attacks and online threats against human rights defenders, anti-corruption activists, environmental activists, and independent journalists have been numerous while investigations into the incidents have been slow, and at times ineffective. As of September, the Institute of Mass information, a watchdog group, recorded 73 cases of obstruction of journalists' professional activities, 17 beatings, 12 threats, and 11 restrictions on access to information.

A suspect in the 2016 killing of journalist Pavel Sheremet was released from detention and placed under house arrest in April, pending trial. One other suspect remains under house arrest, and the third one was released on bail in May 2020.

The investigation into the 2018 killing of activist Kateryna Handziuk has led to prison sentences for five men. However, progress in efforts to charge those allegedly responsible for ordering the attack has been slow.

A February decree by Zelensky led to the extrajudicial banning of three pro-Russia television channels and threatened media pluralism in Ukraine. The decree was based on a law that grants the government authority to sanction foreign individuals and entities that it deems have engaged in activities which could threaten Ukraine's national interests, national security, sovereignty, and territorial integrity.

HATE CRIMES & ANTI-LGBT ATTACKS

►In the first half of 2021, civil society groups reported a sharp increase in attacks against LGBT, anti-corruption, and women's rights activists, including by far-right groups and individuals.

►In May, parliamentary committees began discussing a bill that would increase liability for discrimination and intolerance. In April, the Health Ministry lifted restrictions against gay people on donating blood.

►In May, LGBT activists held a pride march in Kyiv in support of transgender people, under police protection. Far-right activists organized a counter protest but did not attack the march.

►The police prevented attempted attacks on pride marches in Odesa and Kharkiv, held in August and September. In Odesa, the police arrested over 50 people who tried to attack the pride participants. Twenty-nine officers were injured during the clashes.

►In March, members of a far-right group assaulted six participants of the Women's Rights march in Kyiv. Four men have been arrested.

►On May 29, far-right groups disrupted outdoor events in Kyiv and Odessa, held by LGBT rights group Insight.

►Also in May, far-right radicals in Kyiv sprayed teargas at the screening of a film about Ukraine's LGBT community. Twenty people received minor eye burns.

►The LGBT Association LIGA faced threats, online bullying, and attacks in Odesa and Mykolaiv. In May, masked men threw stones at the building of the LIGA's office in Odesa, damaging it.

►Roma people remained a target of online hate speech and occasional physical violence. In April, local media published a video from the meeting of the Ivano-Frankivsk mayor with local police, where he ordered them to "move Roma people back to Zakarpattya."

►No progress has been made in ensuring accountability for the 2017 murder of Mykola Kaspitsky, the leader of Roma community in Kharkiv region. In January the case was closed for the fourth time. Throughout the year, activists raised concerns over the police allegedly sabotaging the case. In January. police broke up two protests against far-right groups, under the pretext of Covid-19 restrictions, while other protests were allowed to go on unrestricted.

►In June, Ukraine repatriated a mother and her seven children held in dire conditions in a camp for Islamic State (ISIS) suspects and family members in northeast Syria. The authorities had repatriated two other Ukrainian women and seven children in 2020.

CRIMEAN PENINSULA: ARRESTS OF CRIMEAN TATARS

Russian authorities in Crimea continued to persecute Crimean Tatars, including by conflating religious or political beliefs as affiliation with Hizb ut-Tahrir, banned in Russia as a "terrorist" organization but legal in Ukraine. Dozens of Crimean Tatars continued to serve prison sentences on arbitrary charges for real or perceived affiliation with the organization—many of them members of the Crimean Solidarity, a group that supports Crimean Tatars arrested on politically motivated grounds. In February and August, a total of 11 men were arrested on similarly spurious claims.
In September, authorities arrested Nariman Dzhelyal, one of the few Crimean Tatar leaders remaining in Crimea, on trumped-up charges of "aiding sabotage." Authorities detained four other Crimean Tatars in connection with the case.

Russian authorities continued to conscript males in occupied Crimea to serve in Russia's armed forces, in violation of international humanitarian law. Conscription was carried out in tandem with enlistment advertising campaigns in Crimea and military propaganda for schoolchildren.

KEY INTERNATIONAL ACTORS

ECtHR: In January, the European Court of Human Rights found a Ukrainian interstate complaint against Russia to be partially admissible. The court recognized that Russia had "exercised effective control" over Crimea since 2014, paving the way for accountability for violations of the European Convention on Human Rights by Russia during its occupation of the peninsula.

EU: In April, the European Union issued a statement formally accusing Russian authorities in Crimea of conducting a conscription campaign, labelling it a "violation of international humanitarian law." The EU also condemned in September the detention of Crimean Tatar leaders and called for the release of Ukrainian citizens detained in Crimea.

UKRAINE'S NATIONAL STRATEGY FOR HUMAN RIGHTS

In May, during their annual human rights dialogue, the European Union welcomed the adoption of Ukraine's recent National Strategy for Human Rights and the Action Plan, while also calling for further progress in reform of multiple sectors and successful resolution of the Maidan and Odesa investigations.

EU-UKRAINE SUMMIT: During the EU-Ukraine Summit in October, both parties reaffirmed their commitment to strengthening the political and economic integration of Ukraine with the EU without a particular emphasis on human rights and the rule of law issues.

BIDEN-ZELENSKY FIRST MEETING

During their first meeting at the White House in August, US President Joseph Biden and President Zelensky committed to upholding human rights in Ukraine, including in such areas as reforming the judiciary, combatting corruption and fighting discrimination against the LGBT community. The presidents committed to holding Russia accountable for abuses in the territories of Ukraine controlled or occupied by Russia and to seeking the release of political prisoners held there.

GERMAN-UKRAINIAN PARTNERSHIP ON THE HORIZON

In Andreas Unland, *Germany Become a Major Ally of Ukraine? Counterintuitive Deliberations on a Coming Partnership between Kyiv and Berlin*, World Affairs, v. 183, Spring 2020, Unland notes that over the last few years, intergovernmental affairs and the roles of individual countries within the West have started to shift. In response, Unland posits, Kyiv should reorder the priorities and emphases of its foreign political, economic, and cultural policies. This re-orientation's central focus should be more resolute than the hitherto deepening of Ukrainian relations has been, not only with the German government but also with the broader political elite, industrial companies, and the civil society of the Federal Republic of Germany. A recent systematic study of German perceptions of Ukraine can help develop new approaches, initiatives, and policies to reach a new level of German–Ukrainian partnership.

EU MEMBERSHIP FOR UKRAINE?

Perspectives of the EU Membership for Ukraine: The Main Challenges and Threats, 2021 Journal of the Human and Social Science Researches

Series/Report no.: DOI: 10.15869/itobiad.880128.

With the entry into force of the Association Agreement between Ukraine and the EU, the relations between Kyiv and Brussels have reached their peak. At the same time, there are numerous challenges and threats that impede the further deepening of Ukraine's integration into the European Union, not the least of which is parked at the border within a few hours from Kyiv.

EU ENLARGEMENT FATIGUE

The intensification of internal disharmony in the EU after the enlargements in 2004 and 2007 have led to an increase of the enlargement fatigue. The aspirations of some European leaders to first regulate the situation inside the EU and only then to consider the prospects for enlargement potentially threaten Ukraine to stay down in the gray zone between the EU and Russia for a long time. The fact that Brussels is continuing a dialogue on enlargement with the Western Balkan countries, however, may be the source for optimism for the Ukrainian side. Citizens of key EU countries consider the high level of corruption and low economic indicators of Ukraine to be the main challenges for the Ukrainian state on its way to membership in the Union. In recent years, despite the ongoing Russian aggression, Ukrainians managed to form an institutional and legal framework to counteract corruption and set the stage for economic growth. This creates grounds for expectations that the impact of relevant negative factors will decrease significantly over time.

THE RUSSIAN FACTOR

The position of Russia is the greatest threat for Ukraine's European prospects. After beginning of the Russian aggression in Ukraine, the leading

states of the world and EU, while implementing foreign policy in the eastern direction, gradually have opted out of the “Russia First” principle. At the same time, the number of achievements of Russian diplomacy in the EU lately confirms that Russia remains one of the key partners of the leading capitals of Europe. The article concludes that now the Russian factor is a major deterrent to Ukraine's EU membership.