alliance for securing democracy
G | M | F

Conceptualizing Foreign Interference in Europe

Kristine Berzina, Senior Fellow
Etienne Soula, Research Assistant
March 18, 2020

Introduction

Europe has been at the forefront of confronting asymmetric attacks from foreign adversaries. Disinformation campaigns have been used against the European public since the Soviet era, and with the advent of social media platforms, they have become a regular phenomenon across the continent. Cyber-attacks have become a frequent occurrence too, particularly since 2007, when Russia conducted a campaign of cyber-attacks on Estonia.[1]

Even so, it was the 2016 U.S. presidential election that accelerated European measures against interference in democracies. National governments across Europe have launched holistic efforts to counter interference. In 2018, France announced the Paris Call for Trust and Security in Cyberspace, which calls for cooperation to "prevent malign interference by foreign actors."[2] Over one thousand national and local governments, civil society, and industry groups have signed on, and multi-stakeholder communities have formed to advance the principles laid out in the Paris Call.

Sweden is applying the concept of "total defense" to educate and protect its population. Sweden's Civil Contingencies Agency sent a booklet to all households in 2018 with guidelines on how citizens should protect themselves from false information and cyber-attacks as well as many other threats.[3] Finland and Latvia are applying the same "total defense" strategy in their own political systems.

Increasingly, European Union institutions are also turning their attention to interference. The newly elected European Parliament passed a resolution in October denouncing foreign electoral interference and disinformation in national and European democratic processes.[4] And European Commission President Ursula von der Leyen has given her commissioners a mandate to protect democratic systems and institutions from "external interference."[5]

Amid this burgeoning activity, however, one thing is missing. There is little consensus on what exactly "interference" is, and how the term "interference" is similar or different from other related concepts, such as "influence." The lack of a common framing of "interference" across Europe can delay or complicate lawmakers' initiatives and muddy civil society's efforts to build awareness and rally opposition against incursions into democratic processes.

Defining interference comes with risk. Policymakers can create a definition that is either too broad,[6] which could inhibit the freedom of expression or put undue burdens on political participation, or one that is too narrow to cover certain forms of malign behavior in a quickly evolving field, inhibiting democracies from protecting themselves because an attack does not "fit" within said definition. Establishing a definition that merely catalogues commonly-used tactics (for example: cyber-attacks, disinformation, economic coercion, and malign finance) would also prove inadequate because any definition of interference should be flexible enough to capture new technologies and approaches. Moreover, a list of tactics fails to explain the underlying factors driving interference activities.

To contribute to the definition-setting debate, this paper addresses why a definition could be helpful for countering interference, lays out the state of play in the EU on defining interference, provides a review of existing government and academic definitions related to interference, and discusses the concept of legality and interference. Finally, this paper suggests two core criteria to assist in the determination of whether any given activity constitutes interference: (i) intent (including the factors of timing, coordination of behavior, and scale of effects), and (ii) transparency. An act does not need to match both criteria to constitute interference, but they are certainly mutually reinforcing.

Why a European definition can be helpful

Interference is a relatively new political term and area of study, and it has not been formally defined by the EU. Despite that, EU institutions are taking new steps against interference. Upon taking up her mandate, European Commission President Ursula von der Leyen expressed concern over the fact that "our democratic systems and institutions have come increasingly under attack in recent years from those who wish to divide or destabilize our Union" and she has called on her commissioners to take action against "external interference."[7]

New efforts to address interference are underway across EU institutions and member states, from investigations into cases of suspected interference,[8] proposals for a special committee in the European Parliament on foreign interference and disinformation campaigns,[9] to debates over regulation of platforms and industries that facilitate the most publicly visible elements of interference (such as disinformation).[10] The biggest stumbling block is the question of scope: what are policymakers talking about when they act against "interference?"[11]

To begin with, the term "interference" has negative connotations. The Cambridge Dictionary defines the term "to interfere" as "to involve yourself in a situation when your involvement is not wanted or is not helpful."[12] Accordingly, interference should not be used to describe benevolent, benign, or neutral nation-state activity beyond its borders.

Policymakers sought to make this distinction clear by adding a qualifier in the case of "malign interference" in the G7 Charlevoix Commitment[13] and the Paris Call, and of "malicious interference" in the September 2018 European Commission Communication.[14] But this is problematic because it suggests there is a form of interference that is not malign. Moreover, the inclusion of the qualifier shows that there is not a common political understanding in the transatlantic space of what the term "interference" means.

The lack of definitions matters for the wider public and policymakers alike. First, it is difficult for policymakers and citizens to take a stand against interference and take necessary countermeasures if there is inadequate clarity on what it is. How do governments distinguish between traditionally-recognized military and intelligence activity from interference involving asymmetric tools if there is no definition? Without a definition, policymakers could view these activities as permissible — even if they are undesirable — and feel constrained to take steps to defend against them. In addition, the EU and member states could find it difficult to impose costs on actors if there is no consensus on how to classify the type of activity those actors are conducting. The lack of a common understanding of what interference is can lead to the conflation of acceptable government activities, such as public diplomacy, with unacceptable acts of interference. A clearer definition can draw the lines of permissibility, protect core democratic values, and give governments the tools to establish norms in this space.

A definition can also give governments — and even private industry — clearer guidelines for permissible and impermissible behavior in new domains, like the digital realm. Citizens, policymakers, and private companies are only beginning to understand how digital practices and technologies are linked to political activity. Some online practices, such as microtargeting for ads, are widely used for benign commercial and political purposes, but can also be abused for nefarious objectives. Other practices, such as hack and leak operations and disinformation campaigns, often have clear malintent.

At the moment, the lack of a standard definition for the concept of interference has led private companies to set inconsistent policies in their terms of service when policing online interference, including disinformation. For instance, the Twitter Rules have extensive guidelines on election integrity: "You may not use Twitter's services for the purpose of manipulating or interfering in elections. This includes posting or sharing content that may suppress voter turnout or mislead people about when, where, or how to vote."[15] But Facebook has its own definitions. Facebook defines "Foreign or Government Interference" as "Coordinated Inauthentic Behavior conducted on behalf of a foreign or government actor."[16] Indeed, unacceptable behavior on one platform could be deemed acceptable on another. The misalignment of stances by Google and Facebook on online political ads in November 2019[17] is but one example. A formal EU definition for interference could provide the platforms clarity for addressing unacceptable behavior in Europe more consistently.

Where the EU stands

While the U.S. and Australian governments usually describe interference as "foreign," EU institutions do not use a common term. European Commission President von der Leyen refers to "external interference."[18] This can be explained by the fact that that the EU's work with non-EU countries is termed "external." Commission staff occasionally refer to "third country" interference. The situation is different in the European Parliament where the term "foreign" does appear in official communications. The European Parliament held debates both on "foreign interference"[19] and on "interference from other countries in our democracies and elections."[20]

The European Council issued conclusions on "Complementary efforts to enhance resilience and counter hybrid threats" in December 2019 that directly address election interference and introduce the term "manipulative interference," though the term is not defined (emphasis added):

> The Council recognises that a comprehensive approach at all levels is needed to address the challenges of disinformation, including interference seeking to undermine free and fair European elections, making best use of all available tools online and offline. This must include monitoring and analysis of disinformation and <u>manipulative interference</u>, enforcement of European data protection rules, application of electoral safeguards, efforts to enhance pluralistic media, professional journalism and media literacy as well as awareness among citizens.[21]

Although the EU has not formally defined interference, several measures have sought to investigate the problem and explain what interference may look like. An October 2019 European Parliament resolution on "foreign electoral interference and disinformation in national and European democratic processes" gave examples of activities that could constitute foreign interference: "foreign interference can take a myriad of forms, including disinformation campaigns on social media to shape public opinion, cyber-attacks targeting critical infrastructure related to elections, and direct and indirect financial support of political actors."[22] But the resolution did not set out a definition beyond the listed modalities, nor did it provide an assessment of how to distinguish between acceptable nation-state influence and interference.

Similarly, the European Commission has assessed the threat posed by many of the activities that are commonly identified as interference, but it has avoided defining the term or providing consistent criteria for unacceptable behavior. The September 2018 Communication on "Securing free and fair European elections," provides a broad explanation of the new threats online activities pose to democratic debate and electoral processes, with a heavy emphasis on the risks of non-transparent online communication and advertising, cyber-attacks, and the misuse of data.[23] The term "interference" appears only once at the end, when the Commission suggests: "All involved actors have to step up their efforts and cooperate to deter, prevent and sanction malicious interference in the electoral system."

Other European institutions have defined various terms in the realm of interference. A European Parliamentary Research Service (EPRS) briefing on "Foreign Influence Operations in the EU" sets out definitions for misinformation, disinformation, hybrid threats, public diplomacy, soft power, sharp power, and the Kremlin's active measures, but this list does not include interference. In the briefing, EPRS Policy Analyst Naja Bentzen argues that "influence can also serve purposes of interference and destabilization" but does not explain what interference itself is.[24]

As the EU considers defining "interference", it will need to address the inconsistencies in referring to the foreign actors and decide whether a particular formulation of "external," "foreign," "third country" is preferable. The formulation should be careful not to unnecessarily inhibit political cooperation between the Member States, but clarity and consistency would make it easier for citizens to understand the crux of the issue. Inconsistency in language could complicate policymaker and public understanding of what interference is.

Furthermore, the EU will need to move beyond qualitative descriptions of interference activities and lists of modalities. Two questions other countries have sought to answer in their definitions of interference — and which could guide EU deliberations — are: "how can we identify an interference activity," which opens the door to a conversation about intent or effect, and "how is an interference activity different from acceptable behavior"?

Notable government definitions for interference

Europe can learn from other democratic countries' efforts to define interference. The United States' and Australia's definitions of "foreign interference" focus on the malign intentions of foreign actors and seek to set out the lines between acceptable and unacceptable behavior. Concern over effects on democratic processes are either explicitly or implicitly featured in these definitions.

In the United States, the Department of Homeland Security (DHS) has defined "foreign interference" as "malign actions taken by foreign governments or actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies."[25] In addition, DHS presents a foreign interference taxonomy that encompasses the following actions: information activities (including new media abuse, traditional media abuse, and cyber activities), trade/strategic investment, coercion/corruption, migration exploitation, and international organization manipulation.

The U.S. approach is grounded in a framework around intent — actions are deemed to be interference if they are "designed to sow discord, manipulate …" (underlining added for emphasis), and definition reinforces the question of intent at the end through the language "for the purpose of undermining the interests of the United States and its allies." The definition is precise, tied to particular features of the democratic process (free discourse/speech, elections, policymaking), and inclusive of the interests not only of the United States but also of its allies. DHS provides the list of possible modalities of interference not as the definition itself but as supplemental information. This makes the definition more durable because modalities can be added without changing the underlying framework.

Australia has a very robust approach for defining foreign interference and for setting criteria to distinguish foreign influence from foreign interference. In a December 2017 speech announcing legislation against espionage and foreign interference, Prime Minister Malcolm Turnbull delineated what constitutes interference: "We will not tolerate foreign influence activities that are in any way covert, coercive or corrupt. That is the line that separates legitimate influence from unacceptable interference."[26] This approach, which boils the concept of interference down to three C's, is both catchy and comprehensive. Because the messaging is so simple, it does a good job of communicating to citizens.

In practice, the Australian approach goes beyond the three C's. Australia's Department of Home Affairs provides additional guidance on how to distinguish between legitimate nation-state influence and unacceptable interference:

> It is important to understand the difference between foreign influence and interference.
>
> All governments, including Australia's, try to influence discussions on issues of importance. When conducted in an open and transparent manner it is foreign influence. These actions contribute positively to public debate and are a welcome part of international engagement.
>
> Foreign interference, in contrast, is activity that is:
> - carried out by, or on behalf of a foreign actor
> - coercive, covert, deceptive, clandestine
> - contrary to Australia's sovereignty, values and national interests
>
> Foreign interference activities go beyond routine diplomatic influence practiced by governments.
>
> They may take place on their own or alongside espionage activities.[27]

The Australian guidance goes beyond that of the United States by arguing it is legitimate for all governments to seek to influence others, but that these efforts need to be open and transparent. Interference hinges on the lack of transparency. This question of transparency runs throughout Australia's approach: the question of transparency is in the three C's — covert activity is not transparent. And in the list of qualities that deem an act as interference, three of four qualifiers are tied to the notion of transparency: "covert, deceptive, and clandestine" activities are not transparent.

Like in the American definition, the Australian guidelines focus on the values and interests of the state. The allusion to "sovereignty" and "values" in the Australian case echoes the U.S. definition's references of the election system and policy development.

Academic definitions: What distinguishes interference from other concepts in international relations?

While "interference" has become a frequently used term in news and media reports, few researchers and academics have tried to define the concept rigorously. Charles Parton, Senior Associate Fellow at the Royal United Services Institute for Defence and Security Studies (RUSI), based in London, offers an interesting take on what might distinguish influence from interference. Parton builds on Malcolm Trumbull's "covert, coercive, or corrupt" test for interference in Australia to examine the Chinese Communist Party's methods of interference. Beyond the Australian criteria, he suggests that criteria for interference should include "some concept about the potential for interference" — meaning whether an action could open the door to interference, such as accepting equipment and investment in the technology sector — and "a lens of reciprocity" that would examine whether "similar activities by UK actors [would] be allowed by the CCP in China."[28] But his analysis stops short of offering a systematic definition or typology for the latter type of interference.

In academic literature, sophisticated criteria have been suggested for determining "unacceptable influence" but not "interference." Although these criteria do not draw a distinction between the terms "influence" and "interference," they are useful frameworks for clarifying the line between acceptable and unacceptable behavior.

Duncan Hollis, Professor of Law at Temple Law School, explores the question of defining criteria for "influence operations." In his assessment, influence operations can be identified by three shared elements: first, "the deployment of some resources" (material, economic, or informational); second, they "deploy resources for cognitive effect;" and third, "the resources are deployed for cognitive purposes to impact a targeted audience — a state's leadership, opinion-leaders, or mass publics — to change or reinforce attitudes and behaviors in ways that align with the [influence operation's] author's interests."[29] Hollis proceeds to differentiate "unacceptable influence operations" from acceptable ones using five characteristics: transparency, extent of deception, purpose, scale, and effects.[30] But Hollis argues that his five criteria are not exhaustive and that they only seek to illustrate a range of possible influence operations.

James Pamment, Senior Lecturer at Lund University, and colleagues created criteria for "diagnosing illegitimate influence" for Sweden's Civil Contingencies Agency. These criteria focus on "information influence activities" rather than on interference in democratic processes more broadly, and as such would not be applicable to other important vectors of interference in democracies, such as economic coercion or malign exploitation of financial channels.

Pamment suggests a three-pronged definition for information influence activities: "Information influence activities are the illegitimate attempt to influence opinion-formation in liberal democracies (legitimacy); they are conducted to benefit foreign powers, whether state, non-state or proxies (intention); they are conducted in the context of peace, war and hybrid threat-or grey zone-situations, i.e. situations of tension that are neither peace nor war (ambiguity)."[31] Pamment argues that while public diplomacy is the "application of legitimate information power," information influence campaigns are illegitimate because of three interrelated moral reasons: "they deceive people," "they exploit vulnerabilities," and "they break the rules that govern constructive open and free debate."[32]

Furthermore, Pamment and colleagues suggest four criteria to determine illegitimate influence, the "DIDI diagnosis:"

- Deception: Legitimate influence is open and transparent about its source, origins and its purpose.
- Intention: Legitimate influence intends to contribute toward a constructive solution, even if the nature of that solution is contested. Although one should assume good will, in cases of information influence activities there is reason to believe that the intent is merely to do harm.

- Disruption: Legitimate influence ends where the disruption to society is disproportionate to or outweighs the potential benefits of that disruption. Strikes and protests for a specific social purpose, for example, constitute legitimate disruption.
- Interference: The legitimacy of engagement in open and free debate rests, at least partly, on being personally affected by an issue. The clandestine involvement of a foreign power in an election, for example, constitutes interference.[33]

Interference is one of the four diagnostic criteria, but it is defined narrowly as a symptom of influence rather than as the larger concept of "foreign interference." Interference here rests simply on having an illegitimate interest in the issue at hand.

There are useful characteristics of the frameworks provided by Hollis and Pamment that can guide policymakers' deliberations in defining interference. Like the U.S. and Australian governments, both explicitly identify deception and a lack of transparency as key criteria (for Pamment, transparency is the element that is missing in cases of deception) and both discuss intent/purpose as core components of a framework for defining unacceptable foreign behavior.

Hollis and Pamment also focus on effects or the scale of disruption to identify unacceptable behavior. While the effect of foreign actors' behavior is significant, it is also a slippery criterion for interference. First, the full effect of any operation is very difficult to measure or determine. And second, determining the effects or scale of disruption poses tough questions: are only successful operations unacceptable influence? Or are all attempts, no matter how small, unacceptable?

A growing body of literature seeks to clarify terminology around information influence operations. In a December 2019 journal article, Alicia Wanless from King's College London and James Pamment distinguish between the terms "propaganda," "information warfare," "information operations," "influence operations," and others and assess the limitations of existing definitions. Their analysis categorizes the terms by operative factors (truth, intent, origin and legitimacy) and explains the main considerations behind these terms.[34] Other articles in the same issue of *The Journal of Information Warfare* explore "cyber-enabled influence operations," "cyber-influence operations," and "(mis)information operations."[35]

Academic literature provides other terms that are helpful for understanding the concept of interference. The field of international relations recognizes several ways in which states can increase their power and influence in the world. Resort to military force or the overt exertion of economic might, for instance through the use of sanctions, fall squarely within what Joseph Nye termed "hard power."[36] The ambiguous and non-kinetic nature of interference places it firmly beyond the scope of hard power. For the same reason, "interference" should be distinguished from "intervention," with much of the literature around intervention focused on some degree of military action.[37]

For Nye, the other face of nation-state power is "soft power," a state's ability to make other states "want what it wants" through attraction rather than through coercion. Since the concept was first introduced, scholars from around the world have sought to apply it to their state's policies. For instance, Chinese academics have sought to portray Confucius Institutes as tools of soft power.[38] Yet, in the case of Confucius Institutes, entities advertised as ambassadors of Chinese culture often serve more subversive objectives on behalf of the Chinese Communist Party. The visa-ban on the director of one of Belgium's Confucius Institutes on grounds of espionage[39] is but the most recent piece of evidence substantiating long-standing suspicions[40] about the entities' more nefarious, even coercive purposes.

Rather than "soft power," a growing body of literature now argues that authoritarian regimes' initiatives to increase their influence beyond their borders could be described as "sharp power."[41] The concept of sharp power is helpful in highlighting the malign intent behind actions that seek to “pierce, penetrate, or perforate the political and information environments of [democratic] countries.”[42] However, as it has been defined, sharp power is too narrow to describe the full range of non-kinetic actions undertaken by authoritarian states to destabilize democracies in the transatlantic space. Crucially, it leaves out actions undertaken in the economic sphere that could constitute interference, such as coercive investments in technology infrastructure.

Another concept often (mis)used in the context of states’ influence-building is “public diplomacy.” Because public diplomacy has an emphasis on open communication,[43] it should not be confused with foreign interference. In a 2014 EU assessment, public diplomacy is “advocated as a more citizen-oriented form of diplomacy than the standard model, that is a form of intercultural dialogue based on mutuality and reciprocal listening stance and where the ‘targets’ are no longer other governments so much as diverse national and global audiences and publics.”[44] The publication formally defines public diplomacy as “the process whereby a country seeks to build trust and understanding by engaging with a broader foreign public beyond the governmental relations that, customarily, have been the focus of diplomatic effort.”[45] Here again, the emphasis on openness and inclusivity differentiates the concept of public diplomacy from interference.

Existing academic literature does not yet provide a consensus definition of interference. The question of how interference is different from influence, and whether there should be a distinction between unacceptable influence and interference, remains unanswered. The absence of clear academic definitions for interference is a notable gap given the pressing need for democracies to make policy to counter attempts by authoritarian adversaries to interfere in democratic societies.

Existing definitions for narrower concepts such as “unacceptable influence” and “illegitimate influence” in the information realm help provide a framework for addressing interference, though these definitions are not as exhaustive or comprehensive as the policy challenge requires. Future policy definitions should take these frameworks into account and distill the more critical elements for a broader definition.

The clarity in academic and policy literature around traditional concepts such “public diplomacy” is very important for policymakers and the broader public. Definitions and explanations of public diplomacy practices should be widely shared to build greater understanding about legitimate behavior in democratic states and how it differs from illegitimate activity.

A discussion on legality

An illegal act committed by a foreign actor in an area pertaining to the functioning of democracy could be constituted as interference. But framing a definition of interference solely around legality is challenging for several reasons.

First, legal frameworks often take time to catch up to the activities in question. As the EU argues, rapidly developing online activities have brought new threats to citizens,[46] and the legal framework for countering these threats — from cyber security to disinformation and artificial intelligence — is not yet in place. The new European Commission will only take up the question of regulation of industry to prevent against disinformation and manipulation of emerging technologies like AI in the coming years. Waiting for a determination that a certain kind of technological attack is illegal before calling it interference would be overly limiting for policymakers trying to respond to it.

Second, legal frameworks often rely on existing laws that do not take into account the unique circumstances of interference operations. For example, certain EU member states have based their domestic legislation against disinformation on prior legal frameworks. Germany’s Network Enforcement Act (NetzDG) requires online platforms to remove "illegal content" or face steep fines. The determination of what is "illegal content" is based on existing laws that define hatred, depictions of violence, and child pornography, defamation, and forgery.[47] A major challenge of this approach is that foreign disinformation or manipulated content "is rarely so overtly inflammatory as to be considered criminal under NetzDG's definition of 'illegal content'" and can encourage online platforms to be overzealous in their content moderation.[48]

International law is equally an inadequate source of guidance. As Duncan Hollis argues with relation to influence operations, "International law offers some ways to regulate certain [influence operations], particularly those that lead to violence. But, for many other [influence operations] — including Russian interference in the 2016 U.S. election campaign—existing international law is not well suited to the task at hand. […] Simply put, I am not sure that international law is suited to regulation at a cognitive level."[49] This is because the "unacceptable influence operations" that he analyzes do not necessarily fit into the legal parameters of "intervention" or meet the high threshold of a "violation of sovereignty" under public international law. The tactics used in interference operations, such as information manipulation, are conducted in a legal gray zone. Therefore, relying on international law as guidelines for regulating against this activity would be inadequate.[50]

Accordingly, while important in the European context, the consideration of legality should not be core to defining interference. Legality in conjunction with the principles of intent and transparency could provide a more robust system for defining interference.

The core elements of interference

The two core elements outlined below — intent and transparency — are common threads in existing approaches to defining interference. These two criteria are not a definition of interference in and of themselves, but provide a useful starting point for setting a definition for interference. They derive from the normative, legal, and academic frameworks discussed above to assess unacceptable nation-state activity.

Importantly, this rubric is applicable to a wide range of interference tactics as the Alliance for Securing Democracy defines them today — cyber-attacks, information operations, malign financial influence, the subversion of political and social organizations, and strategic economic coercion.[51] Helpfully, this rubric also provides a framework for a definition that can incorporate new tactics as technology evolves.

1. Intent

Most existing approaches to determining whether an action by a nation state is unacceptable hinge on the question of intent: what did the foreign actor seek to achieve? Is the intent to harm democratic systems? Is the intent of the action to disrupt, manipulate, damage or erode confidence in democratic organizations, institutions and processes?

The question of intent is central to the U.S. understanding of interference and is explicit in the U.S. definition. Interference is deemed "<u>malign</u> actions … <u>designed to</u> sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets <u>for the purpose of</u> undermining the interests of the United States and its allies" (underlined to identify designations of intent).[52] In the Australian definition, two of the three C's refer to intent: corrupting and coercive.

Intent is implicit in the EU's discussions of interference. The October 2019 European Parliament Resolution refers to interference as "hostile" and "malicious." The European Commission's Communication on securing elections uses similar qualifiers as it rallies action against "malicious interference."

A similar approach exists at the member state level. For example, rather than using the term "disinformation," as the EU does, the French government prefers the term "information manipulation" in order "to highlight the political intent behind information manipulation campaigns as a defining criterion of the phenomenon."[53]

Several additional factors can contribute to the determination of intent: timing, the coordination of behavior, and scale of effect. The timing of an information operation or cyber-attack is important. U.S. Special Counsel Robert Mueller's indictments of twelve Russian intelligence officers argued that the timing of the leak of the hacked Democratic National Committee (DNC) emails in 2016 mattered — it was timed to maximize impact on the Democratic National Convention and give credence to the allegation that the DNC took steps to favor Hillary Clinton's candidacy over her primary opponent Bernie Sanders.[54] Similarly, the leak of hacked emails in the French presidential race in 2017 occurred immediately prior to the election in an attempt to sway the electorate before heading to the polls.[55] The timing in both of these instances helps determine the intent to disrupt the election process. But timing alone is not the sole determinant of interference. Interference operations happen constantly, not just around election campaigns. The Russian state-sponsored troll farm, Internet Research Agency, began targeting American citizens in 2014, well before the 2016 U.S. presidential elections came into focus — and continued to target them long after Donald Trump's victory.[56]

The coordination of behavior is also a significant factor in determining the intent of information operations. Facebook's policy to take down accounts stipulates, "…the use of multiple Facebook or Instagram assets, working in concert to engage in Inauthentic Behavior… where the use of fake accounts is central to the operation."[57] Coordination between these accounts establishes the intent of the operation.

Another useful marker of intent could be the scale of the effect of an attack or operation. Duncan Hollis and James Pamment both discuss scale of effect or disruption in their criteria for unacceptable influence operations. There is value here — the scale of effect could provide indications of how well-resourced a particular operation is and how serious foreign actors are in their efforts to interfere in democracy. But as discussed earlier, measuring effect is problematic, as is measuring scale. An inexpensive and seemingly small online operation can actually have impact beyond its perceived value. It is important for policymakers to note that a big effect can be cheaply procured.[58]

Scale of effect can contribute to an establishment of intent, but by itself is insufficient as a criterion of interference. The Russian military intelligence agency (GRU) hackers who stole the DNC's emails in 2016 first sought to share them through Facebook, but they failed to attract significant attention. Their post was only shared 17 times. Only when WikiLeaks published the information was it shared widely and did it have a bigger effect.[59] Focusing on the scale of the effect, or the scale of the disruption, in determining whether something is interference would suggest that the GRU's failed hack and leak on Facebook could possibly miss the bar. But the intent in both cases was the same — to disrupt the U.S. political process, affect candidates' campaigns, and shape public perception of the candidates.

2. Transparency

A common feature of interference activities is their covert or opaque nature. Foreign governments seek to use covert or non-transparent means to hide their efforts and destabilize a country's democracy. Russia's Internet Research Agency trolls posed as Americans and created 129 Facebook events between 2015 and 2017, in some cases even creating events that could have led to real clashes between citizen groups, such as by planning a "Stop Islamization of Texas" protest across the street from a "Save Islamic Knowledge" event in Houston.[60] If Americans had been aware that these events were organized by Russian government operatives, they would not have been as effective.

The lack of transparency enables interference not only in the information field but across a broad range of asymmetric tactics. This is especially true in the financial space. Citizens and policymakers need full knowledge of the true beneficiaries of investments in their countries and the strategic implications or "strings" attached to economic ties, especially in the case of energy or technology investments. A lack of transparency in these areas can allow foreign actors to subvert another country's political landscape or distort political processes.

Hidden sources of political funding are especially worrisome. Because most countries limit the access of foreign actors to their elections, efforts to evade detections are very complex.[61] In the United Kingdom, Arron Banks, the co-founder of the Leave.EU campaign, was offered the opportunity to invest in gold and diamond mines by a Russian businessman connected to the Russian Ambassador to the U.K.[62] In Italy, prosecutors are investigating the League party's attempts to seek funds through a Russian oil deal.[63] The best way to counter these opaque activities is through greater transparency in the investment sector and in political financing.

In this typology, transparency is a catch-all term that policymakers could invoke to uncover a range of non-transparent activities and address deception. The concept of transparency, and the lack thereof, can be framed in terms of openness or opaqueness. In Australia, the interference test looks for "covert" activity, including deceptive behavior.[64] Duncan Hollis includes both "transparency" and "deception" as measures to determine whether influence operations are unacceptable.[65] And James Pamment focuses on "deception" as a criterion for illegitimate influence.[66]

Approaches to defining interference should highlight transparency rather than deception. Focusing on the importance of transparency can have important normative value. Frequently, the measures to counter interference present negative responses to negative actions: unacceptable content is banned; corrupt political behavior is punished. Yet framing this discussion around transparency changes the narrative from one of prohibition — and the slippery slope of infringing on rights, particularly in the information space — to one of openness and agency. Emphasizing the importance of transparency of online platforms, in beneficial ownership registers, and in political party financing gives citizens greater powers to engage in democratic processes.

Conclusion

The European Union and EU member states are at the forefront of global efforts to counter interference by authoritarian states in democracies. Clear terminology around interference will help Europeans create policies that identify and counter interference threats and strengthen democratic processes. Policymakers will need assistance in approaching the definition-setting process. Although academic definitions provide guidance around key terms like influence operations, sharp power, and public diplomacy, guidance on defining "interference" is limited. Lessons can be drawn from the Australian and U.S. definitions.

As the EU institutions and member states consider this terminology, it is essential for them to remember a few key points. First, interference is inherently a negative term, unlike influence. Adding too many qualifiers to the term "interference" can muddy its meaning. Second, definitions should be wide enough to catch a rapidly evolving set of interference tactics, not only in the information space but also in the economic and cyber fields. Third, two criteria should be central: interference usually entails a lack of transparency and includes the intent to disrupt or erode confidence in democratic processes and institutions.

Global democracies will be looking to the European definition process as a standard setter. When the EU passed its General Data Protection Regulation, the policy was replicated around the world and forced technology giants to bend to the EU's approach. If the EU defines interference, other democratic governments, global initiatives like the G7, private industry, and civil society can use the EU's framing to defend against interference efforts far outside the EU's borders. It matters for the EU to get this right.

Endnotes

[1] For a compilation of over 360 incidents of Russian government-linked interference across European nations since 2000 see ASD's Authoritarian Interference Tracker.

[2] Paris Call For Trust and Security in Cyberspace (2018) *The 9 Principles*

[3] Swedish Civil Contingencies Agency (2018) *If Crisis or War Comes*

[4] European Parliament (2019) Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes, P9_TA(2019)0031

[5] Ursula Von der Leyen (2019) "A Union that strives for more: My agenda for Europe", Political Guidelines for the Next European Commission 2019-2024

[6] Cf. the Australian Parliament's debates on the necessity to define interference for the purpose of protecting free speech and limit an overly expansive definition of national security.

[7] Ursula Von der Leyen (2019) "A Union that strives for more: My agenda for Europe", Political Guidelines for the Next European Commission 2019-2024

[8] Lorenzo Tondo (2019) "Italian prosecutors investigate League over alleged Russian oil deal claims", *The Guardian*

[9] InfoSociety (2019) "The S&D Group proposed a special committee proposal", *Euractiv*

[10] Samuel Stolton (2019) "EU mulls disinformation regulation but admits alert system has 'never been triggered'", *Euractiv*

[11] The transcript of the European Parliament's September 17 debate on "Foreign Electoral Interference and Disinformation in National and European Democratic Processes" is publicly available.

[12] Cambridge Academic Content Dictionary, "Interfere"

[13] G7 (2018) *Charlevoix Commitment on Defending Democracy from Foreign Threats.*

[14] European Commission (2018) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Securing free and fair European elections: A Contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018, Brussels, 12 September, COM(2018) 637 final, p. 9.

[15] Twitter (2019) *Election integrity policy*

[16] Facebook, *Inauthentic Behavior*

[17] Kara Swisher (2019) "Google Changed its Political Ad Policy. Will Facebook Be Next?", *The New York Times*

[18] Ursula Von der Leyen (2019) "A Union that strives for more: My agenda for Europe", Political Guidelines for the Next European Commission 2019-2024

[19] European Parliament (2019) Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes, P9_TA(2019)0031

[20] A debate took place on November 27, 2019 in the European Parliament with foreign interference in the EU as its main focus.

[21] Council of the European Union (2019) Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions, Brussels, 10 December (OR. en) 14972/19.

[22] European Parliament (2019) Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes, P9_TA(2019)0031

[23] European Commission (2018) *Securing free and fair European elections,* COM(2018) 637 final

[24] European Parliament Research Service (2018) *Foreign influence operations in the EU*

[25] Cybersecurity and Infrastructure Security Agency, *Foreign Interference*, U.S. Department of Homeland Security

[26] Malcom Turnbull (2017) "Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017", *malcomturnbull.com.au* website

27. Australian Department of Home Affairs, *Countering Foreign Interference*
28. Charles Parton (2019) « China-UK relations : Where to draw the border between influence and interference?» *Royal United Services Institute for Defence and Security Studies,* p. 3
29. Duncan B. Hollis, (2018) « The Influence of War; The War for Influence ». Temple International & Comparative Law Journal, Vol. 32, No. 1. p.5.
30. Ibid., p. 6.
31. James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, Alicia Fjällhed, (2018) «Countering Information Influence Activities: The State of the Art, version 1.4 ». Swedish Civil Contingencies Agency and Lund University, p. 15.
32. Ibid., p. 15.
33. Ibid., p. 16.
34. Alicia Wanless and James Pamment (2019) "How Do You Define a Problem Like Influence?" *Journal of Information Warfare* 18(3) December 30.
35. Alicia Wanless and James Pamment (20 19) "How Do You Define a Problem Like Influence?" *Journal of Information Warfare* 18(3) December 30.
36. Joseph S. Nye, (1990) « Soft power » Foreign Policy, (80), p.
37. Michael W. Doyle (2015). *The question of intervention: John Stuart Mill and the responsibility to protect.* Yale University Press.
38. Ying Zhou & Sabrina Luk (2016) « Establishing Confucius Institutes: a tool for promoting China's soft power? », *Journal of Contemporary China*, 25:100, 628-642.
39. Jonas Ekblom (2019) « Chinese academic suspected of espionage banned from Belgium », *Reuters*
40. Bethany Allen-Ebrahimian (2018) « China's long arm reaches into American campuses », *Foreign Policy*
41. Walker, Christopher. "What Is 'Sharp Power'?" *Journal of Democracy* 29, no. 3 (2018): 9–23.
42. Ibid.
43. Zhao Huang and Olivier Arifon (2018) « La diplomatie publique chinoise sur Twitter : la fabrique d'une polyphonie harmonieuse » *Hermès, La Revue*, 2:81, p.45-53
44. Professor Isar et al. (2014) *Preparatory Action 'Culture in EU External Relations': Engaging the World: Towards Global Cultural Citizenship,* document prepared for the European Commission, page 20.
45. Ibid., page 136.
46. European Commission (2018) *Securing free and fair European elections*, COM(2018) 637 final
47. William Echikson and Olivia Knodt, "Germany's NetzDG: A Key Test for Combatting Online Hate," Center for European Policy Studies, November 22, 2018.
48. Berzina et al., p. 46.
49. Hollis, p. 14.
50. Ibid, p. 14-15.
51. Kristine Berzina, Nad'a Kovalcikova, Dave Salvo, and Etienne Soula (2019), The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies. Alliance for Securing Democracy.
52. Cybersecurity and Infrastructure Security Agency, *Foreign Interference,* U.S. Department of Homeland Security
53. Jean-Baptiste Jeangène Vilmer et al. (2018) "Information Manipulation: A Challenge for Our democracies", *Policy Planning Staff (CAPS, French Ministry for Europe and Foreign Affairs)*
54. Ella Nilsen (2018) "The Mueller indictments reveal the timing of the DNC leak was intentional", *Vox*
55. Emily Schultheis (2017) "The Macron Leaks Probably Came Too Late to Change the French Election", *The Atlantic*
56. Internet Research Agency Indictment. U.S. Department of Justice. https://www.justice.gov/file/1035477/download
57. Facebook, *Inauthentic Behavior*; Facebook (2019) *How We Respond to Inauthentic Behavior on our Platforms:*

Policy Update

58. Sebastian Bay, Rolf Fredheim (2019) *Falling Behind: How Social Media Companies are Failing to Combat Inauthentic Behavior Online*, NATO Strategic Communications Centre of Excellence.

59. Craig Timberg (2019) "Russian hackers who stole DNC emails failed at social media. WikiLeaks helped." *The Washington Post*, November 13, 2019.

60. Donie O'Sullivan (2018) "Russian trolls created Facebook events seen by more than 300,000 users." *CNN*, January 26.

61. Kristine Berzina (2019) "Foreign Funding Threats to the EU's 2019 Elections," Alliance for Securing Democracy, German Marshall Fund of the United States, October 9, 2018.

62. Kirkpatrick, David D., and Matthew Rosenberg (2018) "Russians Offered Business Deals to Brexit's Biggest Backer." *The New York Times*, 29 June.

63. Alberto Nardelli (2019) "Revealed: The Explosive Secret Recording that Shows How Russia Tried to Funnel Millions to the 'European Trump.'" *BuzzFeed News,* July 10, 2019.

64. Charles Parton (2019) "China-UK relations: Where to draw the border between influence and interference?" Royal United Services Institute for Defence and Security Studies, p. 3
https://rusi.org/sites/default/files/20190220_chinese_interference_parton_web.pdf

65. Hollis, p. 7.

66. James Pamment, et al., p. 16.