Policy Brief

March 2021

The Paris Call and Activating Global Cyber Norms

Bruno Lété

The Paris Call for Trust and Security in Cyberspace is the best available tool for a wide range of actors to interact on the inclusive governance of cyberspace. It is a helpful platform to develop fresh ideas on cyber norms and to feed them into intergovernmental negotiations, like the UN processes, even if it is not formally included in these.

The extent to which the Paris Call will shape the implementation of cyber norms will be defined by the diversity and credibility of its signatories, the future shape of intergovernmental cyber norms negotiations, and the rise of national sovereignty in cyberspace. Its strength is to build bottom-up capacity to implement norms, a fundamental need when providing answers to many of the issues in cyberspace, including concerns around trust, stability, and security.

Its capacity to play this role would be improved by creating a Paris Call Liaison Hub, defining concrete goals for each Paris Call Working Group, creating information-sharing platforms, investing in public awareness, reaching stakeholders in Africa and Asia, and engaging different levels of multilateralism.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

The Paris Call for Trust and Security in Cyberspace[1] issued by France's President Emmanuel Macron in November 2018 calls for all cyberspace actors to come together to face digital threats endangering citizens and infrastructure. It is based around nine principles to secure cyberspace and encourages states to cooperate with private-sector partners and civil society. As of February, 79 states, 33 public authorities, 374 civil society actors, and 688 companies had signed the Paris Call.[2] In doing so they committed to adopting responsible behavior within cyberspace. The question is how to ensure the Paris Call remains a relevant tool to build trust and security in cyberspace.

This brief addresses this question particularly through the lens of Principle 9 of the Paris Call, which concerns international norms and promotes the widespread acceptance and implementation of responsible behavior as well as confidence-building measures in cyberspace. The first section sets out how the international community is attempting to shape responsible state behavior in cyberspace amid the increase in state-driven cyberattacks. The United Nations remain the most important platform to do so but the struggle of governments to find compromise has exposed a need for multi-stakeholder platforms such as the Paris Call. The second section identifies factors that will define to which extent the Paris Call will have influence over the UN processes. These include the diversity and credibility of signatories, the future shape of UN negotiations, and the rise of national sovereignty in cyberspace. The third section makes recommendations to strengthen the Paris Call. It highlights the need to create a liaison hub, to define concrete goals for each working group, to create transparent information chains, to invest in public awareness, and to reach out to new or underrepresented regions, and to engage different levels of multilateralism.

This brief is based in part on the discussions at three off-the-record online roundtables convened by the German Marshall Fund between September and November 2020. These brought together European national and regional politicians, officials from ministries of foreign affairs (including cyber-policy directors and legal advisors), academic specialists in international law, representatives of the IT and non-IT industries, and actors from civil society to discuss the value of the Paris Call to shape international cyber norms, including related debates at the UN.

The 9 principles of the Paris Call for Trust and Security in Cyberspace

Principle 1. Protect individuals and infrastructure
Principle 2. Protect the Internet
Principle 3. Defend electoral processes
Principle 4. Defend intellectual property
Principle 5. Non-proliferation of malicious software and practices
Principle 6. Strengthen digital lifecycle security
Principle 7. Support cyber hygiene
Principle 8. No private hack back
Principle 9. Promote international cyber norms

An Evolving Context

Over the past two decades, rapid advances in computers, software, communications, and sensing technologies have connected billions of individuals across the globe, integrated economies through connected supply chains, and spurred new efficiencies through the Internet of Things. The outbreak of the coronavirus pandemic has accelerated this digital transformation. These advances, however, also bring challenges, including the now nearly absolute dependence of all developed and many developing countries on the integrity of digital networks and systems. Despite the general resilience of network-based systems, deep digital integration has also created vulnerabilities to cyberattacks by individual hackers, organized crime, terrorist groups, and even states. Governments intending harm are perhaps the greatest threat because they can invest large financial, technical, and military resources to developing new cyber

1 See the Paris Call website.

2 See the full list. The German Marshall Fund of the United States did so in 2019.

tools for exploiting vulnerabilities that are inevitable in any complex system.

Such attacks are all too real. Starting with Russia's denial-of-service attacks on Estonia's government and financial system in 2007, they have become more numerous and more destructive. For example, the WannaCry ransomware attack in 2017 affected hundreds of thousands of computers in 150 countries. The 2020 SolarWinds hack targeting government agencies and private companies is considered to be one of the biggest cyberattacks in U.S. history. By one estimate, the world experienced 43 significant cyber incidents in the last quarter of 2020.[3]

Concerns about cybersecurity have skyrocketed. The increased splintering of the Internet along geographic and commercial boundaries, and the lack of international consensus on cyber norms make it easier for governments to engage in malicious digital operations. Establishing rules of the game in cyberspace is therefore more imperative than ever.

The list of national, bilateral, or multilateral initiatives to find solutions to this problem is growing. Last December, the European Union adopted a new cybersecurity strategy aiming at making physical and digital critical entities more resilient. [4] In January, the U.S. State Department launched a new Bureau for Cybersecurity and Emerging Technologies to help lead diplomatic efforts around these issues, while China and Indonesia signed a memorandum of understanding on developing capacity building for Internet security.[5]

However, the United Nations remains the most significant body to define rules of behavior in cyberspace at the global level. Within the UN First Committee, countries entrusted two entities to lead such negotiations: a Group of Governmental Experts (GGE) established in 2004, and a parallel Open-Ended Working Group (OEWG) established in 2018. This helped to define various norms and standards for state behavior in cyberspace, most notably when countries agreed to adopt two groundbreaking GGE reports in 2013[6] and in 2015.[7] But volatile relations on cybersecurity between major powers such as China, the European Union, Russia, and the United States mean that compromise and consensus becomes increasingly difficult to find; the limits of the intergovernmental process to shape or implement norms are being exposed.

In 2013, the GGE recognized the need to think of new cyber-governance practices that include a multi-stakeholder model instead of relying solely on the intergovernmental approach. [8] Cyberspace and state behavior associated with it constitute a complex and interdisciplinary area. It demands policy development that is inclusive and expertise-driven, and which engages a broad range of stakeholders.

Initiatives that extend the responsibility of cybersecurity to non-state actors have proliferated over recent years. Examples include the Global Commission on the Stability of Cyberspace, the Cybersecurity Tech Accord, or the Paris Call. Each is unique in the way it engages stakeholders and develops proposals for norms and policies that enhance stability and responsible state behavior in cyberspace. Many—mostly democratic—governments also increasingly include these initiatives in policymaking.

Adapting to Critical Factors

Since cyberspace became a UN issue in 1998, defining which norms and standards apply has been the prerogative of governments. But growing attention is given to the role of multiple stakeholders in shaping

3 Center for Strategic and International Studies, "Significant Cyber Incidents Since 2006," January 2021.

4 European Union, "The EU's Cybersecurity Strategy for the Digital Decade", December 16, 2020.

5 The Star, "China, Indonesia strengthen ties to develop cyber security capacity and technology," January 24, 2021.

6 United Nations General Assembly, Report A/68/98, 24 June 2013: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/pdf/N1337166.pdf?OpenElement

7 United Nations General Assembly, Report A/70/174, 22 July 2015: https://undocs.org/A/70/174

8 United Nations, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013

responsible state behavior. It is no longer unusual for the UN processes to reach out to a diversity of stakeholders for advice, opinions, or expertise. The GGE has held regional consultations with civil society and the OEWG was given a mandate to hold consultative meetings with industry, non-governmental organizations, and academia. However, having two bodies focus on cyberspace has at times proven to be confusing, and questions remain regarding multi-stakeholder input into the UN or other intergovernmental processes.

In light of this, the Paris Call is a major effort to create a multi-stakeholder structure that is appealing to state actors and to grassroot movements. It seeks to complement intergovernmental negotiations and similar initiatives. It has enjoyed broad support and may be to date the best available tool for a wide range of actors to interact on the governance of cyberspace and to implement norms of behavior. The following factors will define how much the Paris Call will be able to influence state behavior in cyberspace, including its capacity to advance the creation and implementation of norms.

Improving the Diversity of the Paris Call Community

The Paris Call aims for global reach. Its signatories cover diverse sectors and geographies, and it remains open to additional ones. Its legitimacy and value will stand or fall with the extent of its community. All EU member states are signatories, but Africa and Asia are underrepresented. The United States, India, China, and Russia did not sign and their absence sets another limit on the impact of the Paris Call. However, several corporate and civil actors in those countries did sign; for instance, Huawei did so in 2019.

Reaching stakeholders in developing and in non-democratic countries remains a challenge. More capacity-building and resources are needed to reach them. The more numerous and diverse the signatories, the better the Paris Call community will be able to credibly engage the UN or other groupings on cyber norms. In this respect, the value of the Paris Call goes beyond the nine principles—it also has the potential to commit the diverse members of its community to universal values around human rights or the rule of law.

Signatories' Observance of the Principles

There is a risk that the Paris Call signatories—consciously or unconsciously—may not always abide by its principles. As these are not enshrined in international law, it is difficult to apply pressure on signatories to respect the call's standards and practices. Attempting enforcement is unlikely to be the answer because it is difficult to implement from technical and political perspectives. Therefore, compliance is likely to remain voluntary, but this remains unmonitored. There is no mechanism in the Paris Call that allows to push for observance of the principles. Neither is there a tool to map trends in observance and to understand how the principles are diffused in ways that affects behavior in cyberspace. The credibility of the Paris Call for governments, the UN, or future community members will greatly increase if there is certainty that the principles go beyond just word and that its signatories help to accelerate an effective norms regime.

Uncertainty in UN Diplomacy

The future of the UN cyber negotiations is unclear. The latest attempt to expand on the norms that were agreed in 2013 and 2015 broke down in 2017 as a new round of GGE discussions failed to produce a new consensus report. Since then, the GGE and OEWG have been working separately on the same governance issues, with little progress. Last October, 40 countries—a majority of these EU members—endorsed a France-led proposal to end these dual-track talks and to create instead within the UN a more flexible Programme of Action for Advancing Responsible State Behavior in Cyberspace (PoA).[9]

The PoA would split cyber governance into smaller individual issues and to spur action where countries can find agreement. The proposal was shared with a

9 "The future of discussions on ICTs and cyberspace at the UN."

meeting of the OEWG in December where it enjoyed significant support. But so far leading cyber powers such as China, Russia, and the United States have not endorsed the PoA. Instead, shortly after the proposal, the United States and Russia put forward competing resolutions outlining their respective vision on the future of UN negotiations. The U.S. resolution called on states to wait until the current GGE and OEWG meetings are completed and the UN General Assembly later this year decides on any future work needed. [10] The Russian resolution called to renew the OEWG to 2025 with the same mandate.[11] As the PoA was only presented as a recommendation, and its content now contradicts the U.S. and Russian resolutions that were adopted by the UN First Committee, it leaves the idea on thin ice. The uncertainties around the future of the UN cyber negotiations also makes it difficult to gauge how much political support governments around the world will give to multi-stakeholder initiatives like the Paris Call. The outcome of the UN discussions will define what it can credibly achieve.

Increase in Cyberspace Sovereignty

The Paris Call principles are authoritative because they build on norms that have been defined in the UN system and by civil initiatives such as the Global Commission on the Stability of Cyberspace. But for states to adhere to a norms regime they must perceive some real benefits, or at least find it too costly to remain outside. With current UN negotiations gridlocked and no universal agreement in sight how to implement norms, this calculus becomes less relevant because the balance between perceived benefits or cost is not being enforced. The risk is that governments may increasingly take actions that violate norms in order to protect their sovereignty against state and non-state actors that conduct malicious cyber operations. The fact that states ignore norms and show less restraint to unilaterally defend their national interest in cyberspace threatens the Paris Call's core mission of trust-building.

As trust in norms is decreasing, the unpredictability of cyberspace is increasing. The challenge for the Paris Call is to demonstrate that norms may not provide the quick-fix solutions that governments hope for but that in the long run they create a solid foundation for more security and stability in cyberspace.

How to Use Scare Resources

The United Nations remains the best venue for governments to agree on norms of state behavior in cyberspace—and ideally this should be done in the next few years. How the UN processes move forward will determine what kind of role multi-stakeholder initiatives like the Paris Call play. Even if not formally included, the Paris Call will be a helpful platform to develop fresh ideas to feed into the UN processes and beyond. However, greater influence can only come with more resources. The following six actions will help the Paris Call to develop the capacity it needs.

Create a Paris Call Liaison Hub

Perhaps the biggest challenge for the Paris Call is how to connect its community and to leverage the potential of such a vast and diverse group of stakeholders. The way forward can be to create a neutral liaison hub for all signatories. It could be created inside France's Ministry of Foreign Affairs, a main driver behind Paris Call efforts and that plays to a certain extent such a role already. Or the role could be funded and assumed by one or several NGOs that signed the Paris Call. The goal of the hub must be to improve the capacity to implement cyber norms.

In a first stage the core mission of this entity would be to map capacities and resources, and to propose ideas for putting these to more efficient use. This can be achieved if the hub serves as central repository of information, which is now too dispersed, by asking community members to systematically submit their Paris Call projects and initiatives. There should be direct cooperation with other communities—like those of the Tech Accord, the Global Forum on Cyber

10 UN General Assembly, "First Committee Resolution A/C.1/75/L.4."

11 UN General Assembly, "First Committee Resolution A/C.1/75/L.8."

Expertise, or the Global Commission on the Stability of Cyberspace—to collect their information too. The hub could fulfill a matchmaking function between different communities, as well as between projects and donors to focus resources. This would be particularly helpful in regions where resources are most scare. It would rely on the willingness of signatories to share their information but, if successful, the hub would fill a real need in coordination, communication, and capacity building.

In a second stage, more functions could be added to the hub's mission. One could be monitoring and assessing signatories' compliance with the Paris Call principles, advocating the principles to state or non-state actors, and pursuing the enlargement of the community by engaging with new stakeholders.

Creating such a centralized entity would increase the weight of the Paris Call in the implementation of norms-, including vis-à-vis governments, regional organizations, and the UN. A hub can communicate a clear and coherent vision on the principles, publish relevant reports feeding into intergovernmental negotiations (including the GGE and OEWG), and help community members, such as small NGOs or small and medium-sized enterprises, that lack the capacity for high politics to have their voice better heard.

Define Concrete Goals for Each Working Group

The Paris Call is a broad initiative that promotes itself as an undividable package of objectives. This makes sense because signatories cannot simply pick and choose among principles. But this also makes it diffuse and harder to manage concrete goals. Even within each principle there is a great variety of topics to address. To solve this issue France's Ministry of Foreign Affairs announced on March 1 the creation of six working groups.[12] Their aim is to breakdown the Paris Call goals and to pursue the implementation of its principles. Preliminary work and results of these groups will be presented at the Paris Peace Forum in November.

To turn the Paris Call into an effective advocacy tool and yield greater efficiency within the stakeholder community, each working group chair should define objectives that can be monitored, measured, or evaluated over a period of time. Group 1, which focuses on expanding the community of supporters, could set targets for the desired annual percentage increase in the number of signatories. For Group 3, on promoting a multi-stakeholder approach in UN cyber negotiations, the objective could be to pursue a desired number of meetings between the Paris Call community and the GGE or OEWG. And Group 6, on developing practical tools for supporters, could monitor the extent to which these are being used among community members and draw lessons learned. Specialist and smaller issue groups have clear advantages, as the CyberSecurity Tech Accord[13], the CyberPeace Institute[14], and the Siemens Charter of Trust have demonstrated.[15] They provide focused expertise that can be interesting to governments, they carry more weight to influence policy, and they are easier for multilateral organizations like the UN to interact with. But working groups also need concrete goals within their mission. Monitoring or evaluating the influence of the Paris Call is an aspect that is currently underdeveloped. The creation of the working groups is a unique opportunity to create such capacity in a manageable way.

Create Information-Sharing Platforms

Lack of transparency about state behavior is the single most important obstacle to implementing norms in cyberspace. For reasons of national interest, governments are rarely prepared to share information about their cyber activities. The private sector can help to address this issue because it is often the first responder to cyberattacks. The data that companies have make

12 Ministry for Europe and Foreign Affairs, France, "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace."

13 For more information, see CyberSecurity Tech Accord.

14 For more information, see CyberPeace Institute.

15 For more information, see Siemens Charter of Trust.

them a key intelligence player that can drive the political process around norms. Their data can help understand the threat landscape, expose the damage from malicious cyber behavior, and identify victims and perpetrators. But this information is only helpful in implementing norms if it is complemented by government intelligence. This implies that governments also have a responsibility to share their information with the private sector. The result of this cooperation would provide a more complete intelligence picture for legislators, law-enforcement officers, or computer emergency response teams that have a direct stake in upholding existing norms. Moreover, the public and private sectors must work together to inform audiences and raise public awareness for the importance of responsible cyber behavior.

In sum, all sectors must cooperate to promote norms and expose malicious activities. Since it includes such different actors, the Paris Call is a remarkable environment to foster a change of attitude and to launch projects that encourage more openness. Its bottom-up approach is a powerful attribute to counter lack of transparency. For governments, it can provide an environment to share information with actors that abide by the same rules of the game. Information-sharing platforms stimulate trust and serve as confidence-building measures between actors. Reaching this goal will likely be more difficult in countries that show the least readiness for openness, like Iran or Russia. But there are 79 governments that have signed the Paris Call and support this approach. Together with the other community members they represent a considerable force in the pursuit of transparency. More transparency in cyberspace will lead to more predictability, which is part of what the Paris Call aims to achieve.

Invest in Public Awareness

Implementing norms of behavior in cyberspace also involves the public. The Paris Call community has a responsibility to make users of the Internet more aware of the norms that apply. One tool for this is education. Governments can more systematically include cyber norms as a topic in basic and further education. For instance, in Israel the Defense Forces teach students about cybersecurity at a very early stage. Germany is introducing school programs around digital awareness and concepts. By comparison, the role universities can play is still underused, with cyber research programs funded by governments still limited. The private sector is also responsible, especially when it comes to the diffusion of information to a larger public. For example, in 2019 Microsoft disclosed that several accounts associated with a U.S. presidential campaign had been targeted by a group linked to Iran's government.[16] This generated significant discussion and media coverage, putting the spotlight on the damage that can be done when states engage in malicious behavior.

Talking publicly about attacks by state actors is an important part of deterrence but companies and governments are often still hesitant to do so. Furthermore, proper cyber education is the basis to inspire civil society to work on these issues. Grassroot initiatives can assist the private and public sectors in raising awareness among Internet users and increase capacity. The Paris Call community should continue to invest in projects that raise awareness around norms; for instance, through conferences, social media, and other tools of communication. This is the best way to spread better understanding of the value of global norms negotiations, like the UN processes, and to ensure fresh ideas from all levels of society feeds into these.

Reach Stakeholders in Africa and Asia

The Paris Call needs global representation to ensure that its principles support and are promoted by everyone. There is, however, a gap in the geographic spread of signatories, with Africa and Asia particularly underrepresented. Many countries in these continents are developing, their demographics are youthful, most endorse a democratic political agenda, and their security conditions are improving. These trends result in

16 Tom Burt, "Recent cyberattacks require us all to be vigilant," Microsoft, October 4, 2019

better digital infrastructure providing millions with new access to the Internet. The challenge is that most governments in Africa and Asia are still behind on norms acceptance and implementation.

But change is on the horizon. At the 2018 ASEAN Ministerial Conference on Cybersecurity, member states agreed to subscribe to the principles recommended by the 2015 GGE report. Singapore hosts a new Cybersecurity Centre of Excellence to help foster technical cybersecurity capacity-building.[17] Fifty-five African Union member states have endorsed a Digital Transformation Strategy that includes priorities for cyber capacity and awareness building.[18] Last November 2020 the Global Forum on Cyber Expertise and Microsoft announced an investment partnership in cyber capacity for Africa.[19]

New stakeholders to widen the Paris Call community could be reached through regional multilateral fora, local grassroot movements, or local conferences and events. The more global the call becomes, the more legitimacy it will have with the UN and other bodies shaping state behavior in cyber space. Having more African and Asian signatories would be a force for good for the international norms debate.

Engage Different Levels of Multilateralism

The United Nations is unique because it convenes the full spectrum of global views and interests. But there are other international organizations and smaller groupings of countries that can be engaged by the Paris Call community to indirectly influence the UN processes and to advance the debate of norm creation and implementation. These gather diverse key players, their structures are more flexible, they possess a credible level of expertise, they often have more experience working with non-state actors, and they carry enough weight to negotiate on an equal footing with big countries like China or at the UN level. Projects can be developed in smaller bodies and then more easily transferred to the UN. The EU, ASEAN, the Organization for Economic Co-operation and Development, or the Organization for Security and Co-operation in Europe are experienced in working with multiple stakeholders and are a good place to engage in policy experimentation and vetting. NATO could offer a good platform to introduce new ideas around a transatlantic zone of cyber stability.

The Paris Call community should also look at relevant geographic clusters. This would make it easier to identify local attitudes and policy goals, and to create projects of common interests. Initiatives could, for example, feature regions with exemplary cyber behavior as a role model or connect cluster of countries with other clusters and assist them in implementing norms of responsible cyber behavior. The goal would be to build an ever-increasing number of geographic pockets of cyber stability. A good example of this is how the Baltic states cooperate on cyber-hygiene initiatives in the public sector and exchange best practices. There have also been efforts between the EU and the United States to strengthen cooperation on the global norms debate, despite the U.S. government not having signed the Paris Call yet. In other words, to act globally the Paris Call also must think regionally.

Conclusion

The Paris Call for Trust and Security in Cyberspace should appeal to any actor dedicated to advancing global cyber norms. Its nine principles are in line with cyber norms identified by the UN and similar initiatives, it offers a source of diverse ideas, it builds acceptance for responsible cyber behavior inside societies, and it accelerates the implementation of cyber norms at the grassroot level. The extent to which the Paris Call can mobilize the international community also makes it a natural partner to the United Nations' norms processes. It has a real potential to complement the UN by being able to act where the UN cannot,

17 Christy Un, "It's time for the Asia-Pacific to move to regional cyber norms," The Diplomat, October 14, 2020.

18 African Union, "The Digital Transformation Strategy for Africa (2020-2030)," 2020.

19 Global Forum on Cyber Expertise, "GFCE and Microsoft announce an investment partnership in Cybersecurity Capacity Building in Africa," November 2020.

especially by operationalizing the existing norms regime.

Despite many uncertainties around the future of UN negotiations, the norms already adopted by the UN and the Paris Call principles provide solid guidelines to shape responsible state behavior in cyberspace. A priority for the Paris Call is now to find the capacity and the resources needed to operationalize the existing framework. The vast diversity of stakeholders engaging in the debate on cyber norms and the proliferation of initiatives that seek to operationalize these norms have set in motion a trend that will be hard to reverse. Governments may still have the prerogative to define the rules of the game but the decisions they make will have far greater impact if they also involve non-governmental entities. Shared responsibility in cyberspace is no longer an alien concept and the Paris Call community is instrumental in accelerating this change. The commitment of over a thousand signatories can only advance trust and security in cyberspace and become a force for good to be reckoned with from the local level to high politics at the UN.

About GMF Digital

Bruno Lété is as a senior fellow at The German Marshall Fund of the United States in Brussels. He provides analysis and advice on trends in geopolitics and on international security and defense policy. He focuses primarily on NATO, developments in Central and Eastern Europe, and cyber security.

This publication is the product of a partnership between The German Marshall Fund of the United States and Microsoft.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org