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

Policy Brief

| Security and Defense Policy |

2017 | No. 38

EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions

By Bruno Lété and Piret Pernik

EU–NATO cooperation in this time of global crisis is increasingly important. In the field of cybersecurity and defense the past years have indeed been pivotal. These issues have long been part of EU and NATO calculus but have only recently moved to the top of their agendas.

Both institutions will continue to face new cyber challenges, and they still find themselves maladapted to the new security environment. The EU and NATO must assert their credibility in cyberspace as strong powers in the eyes of their members and partners — and antagonists.

The EU and NATO are targeted by the very same vectors, notably by cybercrime syndicates, politically motivated non-state actors, and sophisticated state actors. These hostile cyber activities undermine all levels of society in EU and NATO countries, threatening civil, political, economic, and military security. Even though cyber-attacks are a very real threat, much of these activities go undetected, unacknowledged, or inadequately addressed by decision-makers. Stakeholders in various sectors are becoming more informed and engaged around cybersecurity and cyber defense issues, but the challenges remain daunting.

In this context, the Estonian Presidency of the Council of the European Union convened a flagship conference to stimulate new thinking on EU–NATO cybersecurity and defense cooperation in November 2017. This brief summarizes the discussions and offers recommendations to address the most pressing issues on the EU–NATO cyber agenda.

Responses to Cyber Insecurities

Cybersecurity and defense have long been part of EU and NATO calculus but have only recently moved to the top of their agendas. The game first changed for Europe in 2007, when cyber-attacks in Estonia forced both institutions to think more seriously about this type of threat. As a result NATO developed in 2008 its very first Cyber Defense Policy.[1] Five years later, the EU followed suit by adopting its first Cybersecurity Strategy.[2]

1 Cybersecurity was put on NATO's political agenda at the Prague Summit in 2002, but no policy resulted until 2008.

2 European Commission, Digital Single Market News, "EU Cybersecurity Plan to Protect Open Internet and Online Freedom and Opportunity — Cybersecurity Strategy and Proposal for a Directive," February 7, 2013.

The 2014 crisis in Ukraine was Europe's next big shock. Russia's annexation of Crimea and semi-clandestine military actions returned new urgency to European defense and deterrence, but also to cyber-defense and readiness as Russia's hybrid aggressions against Ukraine included cyber-attacks.[3] Since then, NATO and the EU have intensified their initiatives in the cyber sphere. NATO endorsed an enhanced cyber defense policy and action plan in 2011, and it decided to operationalize cyberspace as a domain of defense policy and planning in 2016. That same year all Allies also made a Cyber Defense Pledge to enhance their cyber resilience as a matter of priority.[4] The EU for its part made the fight against cybercrime one of the three pillars of the European Agenda on Security, and recognized cybersecurity as one of the priorities for the Global Strategy for the European Union's Foreign and Security Policy. In 2017 the EU adopted a "Cybersecurity Package" including the revised Cybersecurity Strategy.[5]

In this climate of urgency the EU and NATO have started to see each other as complementary partners to build up their cyber resilience. In order to foster operational level information sharing, NATO and the EU signed a Technical Arrangement on Cyber Defense in February 2016 between NATO's Computer Incident Response Capability and the EU's Computer Emergency Response Team. The most significant step was made with the signing of the EU–NATO Joint Declaration of July 2016 that creates a concrete framework for cooperation in security and defense. With regard to cyber, the implementation plan of the EU–NATO Joint Declaration recognizes four areas of cooperation: integration of cyber defense into missions and operations; training and education; exercises; and standards.

EU–NATO cooperation in times of crisis is increasingly becoming a must. And in the field of cybersecurity and defense the past years have indeed been pivotal.

Three Challenges to Better Cooperation

Despite political-level agreement to work together, EU–NATO cyber cooperation remains difficult and the institutional options often limited. There are three key obstacles preventing the two organizations from cooperating effectively.

Lack of Shared Situational Awareness and Information Sharing

A key condition for fostering credible deterrence in cyberspace is the ability and willingness to respond to malicious cyber-attacks. While the decision to attribute cyber-attacks is in the purview of individual nations, a collective response and deterrence are only possible among countries that have a similar perception of the threats and willingness to respond and risk further conflict. Today there is no shared situational awareness on cyber threats across the EU and NATO member states, despite the clear need to respond jointly.

Furthermore, member states do not all have the same information. Governments are reluctant to share threat intelligence, technical information about cyber incidents, and information about their vulnerabilities and preparedness. (Currently, declarations of EU and NATO member states about cyber capabilities are voluntary, and incomplete.) Cyber threat intelligence is often classified, and there is no immediate channel for classified information sharing between the EU and NATO. The EU does not have a culture of securing information, and NATO often shows little willingness to share classified information with the EU. Moreover, member states that have the technology and capabilities to attribute cyber incidents are often unwilling to share specific details with others. All of this makes issues such as attribution or response to cyber incidents much more difficult — and a common response even more so.

Uneven Levels of Preparedness and Cyber Resilience

Cybersecurity and defense efforts are centered at the national level. Despite the clear mandate of the EU and NATO to help coordinate national efforts, the effective output remains limited because EU and NATO recommendations to member states are

3 Attackers disabled numerous news and other websites using denial-of-service attacks (DDoS).

4 North Atlantic Treaty Organization, "Cyber Defense," Updated November 10, 2017, https://www.nato.int/cps/en/natohq/topics_78170.htm.

5 Joint Communication to the European Parliament and the Council," JOIN, 2017: 0450 final.

non-binding. As a result there is a significant gap across member states in both civilian and military cyber capabilities. Moreover, there is little coordination to ensure national cyber capabilities are interoperable, complimentary, and reinforcing wider EU or NATO efforts. EU or NATO member states that are in need of increasing their national resilience remain skeptical about the EU or NATO providing external assistance that fits their national needs, and are often unwilling to ask for help from the supranational level because of the information sharing issues mentioned above.

No Joint Cyber Exercises, Training, and Education

In their history, the EU and NATO have only held one military joint exercise in 2003. The exercise prioritized conventional priorities and did not include cyber assets. The EU and NATO planned, but failed, to implement more exercises in 2007, 2010, and 2014. Even today, despite the new political momentum in EU–NATO relations, exercises are still conducted separately, also in cybersecurity and defense. Though there is improved coordination between flagship crisis management exercises, such as EU PACE17 or NATO CMX17, they still constitute separate efforts. Organizing exercises in parallel, or with an option for mutual participation, does not go far enough to create a mutual culture of trust and understanding. Moreover, existing EU or NATO table top exercises at the political strategic level are not sufficiently linked to the technical cyber level, which is an important disconnect with crisis response in reality.

Getting Ahead of the Evolving Threat

The task now for the EU and NATO is to find consensus around how to approach and limit cybersecurity threats. Transatlantic cooperation is key to more effectively prevent, detect, and deter cyber-attacks, as well as to hold the perpetrators accountable. As such, the EU and NATO must continue to think how to deepen and widen existing cooperation in cybersecurity and defense. The following recommendations are not necessarily implementable tomorrow, but they are achievable. We offer some ambitious goals to work toward, envisioning what the EU and NATO "should" do, not only what they "can" do, within current political realities.

Develop a Joint Cyber Threat Analysis Hub

The European Union and NATO have already demonstrated their ability to work together in joint-structures, most recently through their support for the European Centre of Excellence for Countering Hybrid Threats in Helsinki. Creating an EU–NATO Cyber Threat Analysis Hub could be another significant step toward institutional cooperation. The first task of the Hub would be to monitor and analyze technical level early-warning indicators on cyber threats and provide enriched output for operational and strategic levels. The Hub would leverage capacities provided by relevant EU and NATO institutions, as well as the private sector. Clearly, it will not be easy to bring these actors together. Nonetheless, this structure would be the ideal for building a shared civilian-military, public-private, and EU–NATO situational awareness. Such a hub would bring together all-source information (open-source, anonymized, and sanitized information from public and non-public sources, including classified ones), and analyze it to foster shared situational awareness. Operational level incident situation reports from EU and NATO entities should be shared in the Hub, and it would have a central role in sharing strategic level reports in case crisis response mechanisms are activated by the EU or NATO.

"Transatlantic cooperation is key to more effectively prevent, detect, and deter cyber-attacks, as well as to hold the perpetrators accountable."

The Hub should act to improve information sharing, by developing technical and operational level Standard Operating Procedures (SOP) for information exchange between the EU and NATO entities. The Hub could also facilitate both informal ad hoc and formal regular information sharing and enable secure lines of communication to share confidential cyber intelligence. As a first trust-building measure for better information sharing, the Hub could therefore help define what type of information needs to be shared, who needs to receive it, when the information needs to be shared, and make sure the information is released in a timely and appropriate manner. An

important function in this respect would be to align technical cyber incident information (from CSIRTs) with military intelligence threat assessments.

Create Joint Committee for Cyber Research and Technology Innovation

Innovation by the private sector in new cyber technologies is outpacing that of governments, and capacity gaps between governments are also vast. The EU and NATO should create a Cyber Innovation Committee to help address the technology gap between the public and private sectors and reduce the uneven preparedness among member states. The Committee would consist of EU and NATO civilian and military officials, researchers, experts, and technology entrepreneurs, whose task would be to look at the private sector market and identify the innovative tools that are relevant to member states. The Committee would complement the efforts of countries that have already set us similar taskforces at national level, or assist the majority of EU/NATO member states that do not have such capacity.

> *"Automated sharing of security and threat information could help the EU and NATO to standardize their threat information."*

Two fast-developing technological areas would be worth keeping track of. First is the growing issue of cloud computing (and cloud backups) for NATO and EU cyber resilience. On the one hand remote storage can help maintain digital continuity of operations in case of an infrastructure disruption. On the other hand, clouds also have their insecurities and the level of responsibility that private operators bear for the security of their cloud still needs to be better defined. In any case, cloud computing is increasingly finding its way into our everyday lives, the EU–NATO Cyber Innovation Committee should look at better cyber defense capabilities in this field. Second is the growing role of automated information sharing in identifying relevant information more quickly, but also in automating threat mitigation in real time. Automated sharing of security and threat information could help the EU and NATO to standardize their threat information. The Committee could identify adequate information-sharing platforms that can withstand increasingly complex attacks, based on open industry specifications. Such platforms not only enable rapid communication and peer-based sharing, they also help reduce cost and increase the speed of cyber defense by automating processes that are currently often performed manually.

Establish a Joint Working Group to Synchronize EU and NATO Crisis Response Systems

To date the existing capacity to synchronize EU and NATO cyber crisis response mechanisms is limited. It involves formal and informal meetings between the North Atlantic Council and the EU Political and Security Committee, exchanges at ministerial meetings, cross briefings to respective Committees and Councils, and informal staff-to-staff interaction, for instance between the European External Action Service and NATO's International Staff. As is true for all forms of collective response in the EU or NATO and especially between the two, better and smoother cooperation in the case of cyber crises would be needed. The EU cyber crisis response mechanisms and NATO's Crisis Response System should be synchronized in order to respond to major cyber incidents that affect multiple EU member states and NATO Allies or EU/NATO institutions. The recent EU announcement of a "blueprint" to respond to large-scale cybersecurity incidents invites rethinking EU and NATO coordination on this issue.

Hence, the EU and NATO should consider establishing a joint working group to propose how to synchronize their systems. As a first step, the Joint Working Group should develop a common template of crisis management phases through the full spectrum of EU and NATO competencies for cyber aspects. The Joint Working Group could also look at clarifying responsibility at the national and supranational levels, for issues like attribution or countermeasures. Proposals should also be made on how to synchronize joint strategic communication among EU and NATO institutions. Finally, more concrete proposals could be developed for using the EU Permanent Structured Cooperation (PESCO) or NATO structures to create national Cyber Defense

Rapid Reaction Teams for supporting countries before, during, and after crises. PESCO could provide the possibility of jointly funding rapid reaction capacities for assisting member states in need. Given the existence of different crisis management tools that the EU and NATO have at their disposal, what is crucial now is to align those instruments and to work toward a common EU–NATO playbook on how to react to cyber incidents and crises.

Develop a Peer-Assessment Process to Identify Key Resilience and Capability Gaps

Cybersecurity and defense are national responsibilities of the EU and NATO member states, and the coordinating role at the supranational level is still limited. The result is an uneven preparedness among member states. The overall consequence of this gap, since our systems are heavily interdependent, is less cybersecurity for all.

NATO has adopted the Cyber Defense Pledge that aims to improve NATO Allies' national cyber defense capabilities in key areas. In parallel, the EU Directive on the security of network and information systems (NIS Directive) forces member states to adopt legal measures to boost the overall level of their cybersecurity by May 2018. The timing may be right to develop a peer-assessment process within NATO and the EU to address key gaps in the cybersecurity and defense of NATO Allies and the EU Member States. Given sensitivities around information sharing, such a process would probably have to be voluntary to start, perhaps following something of a PESCO model, but should aim to soon be broad and comprehensive.

The peer-assessment process would map functions of essential services that are critical for the EU and NATO missions and operations and for member states' national security, as well as their cross-border and cross-sectoral interdependencies. The assessment would produce check lists of vulnerabilities and suggested fixes in participating EU and NATO member states, including their critical economic sectors. One option, among others, could be to use common funding to assist those member states where serious resiliency gaps have been identified, or at minimum, to facilitate voluntary assistance from more advanced nations to those who have invested less in cybersecurity. The EU's Permanent Structured Cooperation (PESCO) could enable member states to transfer from a strictly voluntary resilience and defense capability-building model to a model of binding commitments. The EU and NATO could also strive, together with able and willing member states, to share best practices and make concrete proposals on how to improve civil-military cooperation and public-private cooperation at the national level.

Create a Joint EU–NATO Cybersecurity and Defense Exercise

To date, there are in general no regular, jointly organized exercises between the EU and NATO, despite the fact that these are key for the EU and NATO to better understand each other's institutional processes, to develop common responses, and to cultivate a culture of trust. The creation of a major, annual EU–NATO cybersecurity and defense exercise could jump start more cooperation. Such an exercise could replicate a theoretical joint EU–NATO command and control center and invite EU and NATO staff to coordinate actions of the Union and the Alliance in responding to a large-scale cyber incident as part of hybrid crises. The focus should be on finding solutions in three areas where EU–NATO cooperation remains contentious: common situational awareness, efficient collective decision-making, and civilian-military information sharing.

> *"The focus should be on finding solutions in three areas where EU–NATO cooperation remains contentious."*

The Joint Exercise should also have the objective of cultivating a culture of sharing confidential and classified information and of building trust for information sharing between NATO and the EU. The aim should be to link live-fire technical level exercises to live strategic and operational level exercises, including the most senior officials of the EU, NATO, and member states. A truly innovative element would also be to develop scenarios for the use of offensive cyber capabilities to support the execution of EU and

NATO missions or operations. So far EU and NATO exercises have been limited to the scenario of cyber crisis response, and did not escalate to full armed conflict against another state. But as attitudes toward offensive cyber capabilities are increasingly shifting, there is an opportunity to use an EU–NATO Joint Exercise to develop offensive doctrines as well.

The place to host an EU–NATO Joint Exercise could be the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn that could offer a neutral platform, as well as its expertise and experience in planning and organizing cyber exercises. The lessons learned from the Joint Exercise should be shared with EU and NATO staff, the North Atlantic Council, and the EU Political and Security Committee and with stakeholders in national capitals. The lessons learned should also help align training and education objectives and requirements for EU and NATO staff and militaries.

Study the Adequacy of Cybersecurity and Defense Concepts and Strategies

EU or NATO planning is inwardly focused, revolving around member states' existing capabilities and institutions, while their adversaries often plan their capabilities around the specific vulnerabilities of the actors they expect to confront. Russian "active measures" in Europe and North America, for example, are designed to exacerbate political tensions and vulnerabilities, such as ethnic relations, regional separatism, or socio-economic or cultural cleavages. In this manner, Russia views the development of cyber capabilities as supporting a broader set of conventional, hybrid, or nuclear capabilities. In this light, there is a real need for the EU and NATO — or an independent academic institution — to take a more outwardly focused approach to studying the cyber strategies and capabilities of NATO and the EU's potential adversaries or competitors, such as Russia or China, and that puts in perspective the EU and NATO's own state of play in cyberspace. Such an outward-looking approach toward cybersecurity and defense could serve as a source of inspiration on how to improve EU and NATO cyber strategy and capabilities. As a modern state-on-state conflict is increasingly likely to begin in cyberspace, the EU and NATO must think more actively which cyber capabilities they must develop to more effectively deter — or even retaliate against — their potential adversaries.

Develop EU–NATO Triggers for a Joint Response to Cyber-Attacks

Leaders in EU and NATO member states are getting more comfortable talking openly about active and reactive joint responses to adversaries in cyberspace. NATO has already recognized a serious cyber-attack as a potential Article 5 trigger, and at its November 2017 defense ministerial, the Alliance announced the creation of a Cyber Operations Center that will facilitate the integration of cyber capabilities with conventional military capabilities. But the current doctrine and crisis management conditions enshrined in NATO and EU cyber policies still puts the emphasis on a defensive posture only. A clearer definition is needed of the circumstances, degree, and manner in which active or counter-measures can or should be taken if EU–NATO member states perceive a cyber threat or suffer a cyber-attack.

> *"The Kremlin has been focusing its efforts in the gray zone, and it has gained some sophistication in avoiding lines that would trigger a common response from EU or NATO member states."*

The authorization to use the EU civilian toolbox or NATO offensive capabilities may be clear if a member state faces a large-scale, devastating cyber crisis. The grey zones are a problem. The Kremlin for instance has clearly been focusing its efforts in the gray zone, and it has gained some sophistication in avoiding lines that would trigger a common response from EU or NATO member states. Russia is also not the only potential adversary capable of similar tactics.[6] There is thus an acute need to define when and how the EU and NATO must respond against the day-to-day cyber intrusions that fall below the threshold of being perceived as a clear act of aggression.

6 For example, small to medium scale cyber-attacks on critical infrastructure, hacking of sensitive information, spreading of disinformation.

The development of a set of EU–NATO basic principles that would trigger a joint response would be a good first step. The Tallinn Manual published by the NATO CCDCoE could offer inspiration on how the EU and NATO can define these principles while respecting the application of the international law.[7] Currently the EU and NATO need to assess each individual cyber threat or cyber-attack on a case-by-case basis without the support of standard measurement tools and indicators that can help them formulate a swift and proportionate response. This considerably slows down the decision-making process. Having a set of pre-agreed basic principles would contribute significantly to efforts at improving reactiveness and resilience at the EU and NATO levels.

Create a Joint Cybersecurity Trust Fund to Build Up Resilience of Partner Countries

EU–NATO cybersecurity and defense cooperation with partner nations is a win-win for all sides. Partner nations with the support of the EU and NATO can enhance their own technical cyber capabilities, information networks, and standards, while in return these partners will be able to more efficiently share with the EU and NATO their firsthand information, expertise, and experience. Indeed, the better the technical capacity that partner nations develop, the more they can contribute to EU or NATO collective cybersecurity and defense. A Joint EU–NATO Cyber Trust Fund should be created to address the buildup of local skills, and enable stakeholders in partner nations to attend EU or NATO cyber courses, seminars, trainings and conferences, or to organize similar types of activities in their home land. The Trust Fund can also stimulate the development of local skills by requiring at least one local partner or support team to be involved in the project, rather than simply helping European or American contractors export their technology to the partner nations.

The Joint EU–NATO Cyber Trust Fund should encourage partner nations to propose projects themselves, rather than the EU and NATO pre-defining specifics for trust fund projects and proposals. Bundling the efforts of various EU or NATO assistance providers into a Joint Trust Fund would also avoid duplication and better respond to the real needs of partner countries. Today, decision-makers both in the EU and NATO are increasingly concerned with creating the most efficient capabilities and funding schemes for their partners. There are already genuine examples where the EU and NATO coordinate their financial assistance, such as the regular EU contributions to NATO trust funds for the disposal of unexploded ordinances and anti-corruption. In this light, the development of a Joint EU–NATO Cyber Trust fund may not be such a far-fetched idea.

Lead Application of International Law and Development of Global Norms Around State Behavior in Cyberspace

If the EU and NATO aim at a fruitful cooperation, they need to agree on which norms and rules of behavior are valid in cyberspace, what triggers the right for "digital self-defense," and what forms of action are permitted under the common defense commitment. National laws governing cyberspace are either absent, vague, or difficult to operationalize. The lack of international understanding and conventions complicates efforts to manage cross border cyber-threats. As such, the EU and NATO, as two rather like-minded bodies with overlapping membership, should agree on what the rules of the road for responsible nation state behavior in cyberspace should be. Deterrence only works within a sufficiently shared normative framework. Building on existing proposals for responsible state behavior in cyberspace, the EU, NATO, and their member states have a responsibility to remain open minded for global initiatives at UN level, or to look at ideas emerging from the private sector that advance transparency and accountability about state

> *"Lack of international understanding and conventions complicates efforts to manage cross border cyber-threats."*

7 NATOP Cooperative Cyber Defense Centre of Excellence, "Tallinn Manuel Process," https://ccdcoe.org/tallinn-manual.html.

behavior in cyberspace.[8] The transatlantic partners should lead the way politically by first setting some rules they can agree to, such as a global consensus that commits governments to not only abstain from cyber-attacks that target civilians, the private sector, or critical infrastructure, but that also requires governments and the private sector to work together to detect, contain, and respond to such events — and, to the extent possible, establish some practices and norms for transparently attributing cyber-attacks.

Adapting Together

The accelerating change of the digital age is placing new pressures on top of long-existing coordination difficulties of the EU and NATO. Both institutions will continue to face new cyber challenges, and they still find themselves maladapted to the new security environment. The EU and NATO must assert their credibility in cyberspace as strong powers in the eyes of their members and partners — and antagonists. To achieve this result, NATO and the EU will need to continue to improve their joint force-multiplying functions, their cyber capabilities, to design common command and decision-making structures in cyber exercises, crisis and conflicts, and enhance their interoperability with partners in cyberspace. The security challenges of today require quick responses, necessitating flexible policy frameworks in which coercive reactions can be decided upon among networked actors. EU–NATO cybersecurity and defense cooperation must continue to adapt in a world that is constantly, and rapidly, evolving.

8 See for example, United Nations, "Report of United Nations Group of Governmental Experts on responsible State Behavior in Cyberspace," UN Doc. A/70/174, July 22, 2015; "G7 Declaration on Responsible States Behavior in Cyber Space," Lucca, APRIL 2017.

The views expressed in GMF publications and commentary are the views of the author alone.

About the Authors

Bruno Lété is a senior fellow for Security and Defense Policy in the Brussels office of The German Marshall Fund of the United States.

Piret Pernik is a research fellow at the International Centre for Defence and Security in Tallinn. Her research focuses on cybersecurity and defence issues, including strategies, policies, capacities, and activities of various actors in cyberspace

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

About ICDS

International Centre for Defence and Security (ICDS) is the leading think tank in Estonia specializing in foreign policy, security, and defense issues. The aim of ICDS is to be the regional knowledge hub of first choice for the security and defense communities of Estonia, its allies, and partners. ICDS's mission is to strengthen Estonia's security and defense sector, sharpen strategic thinking in NATO and the EU on security issues that affect the Nordic-Baltic region, contribute to enhancing Estonia's intellectual role within NATO and the EU, and raise public awareness and stimulate public debate on security, defense and foreign policy matters. In addition to conducting research, ICDS organizes the Lennart Meri Conference, the Annual Baltic Conference on Defence, as well as regular national defense courses, and publishes a monthly foreign affairs magazine *Diplomaatia*.

RKK ICDS

RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

1744 R Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@gmfus.org
http://www.gmfus.org/