France's response to Resolution 73/27 "Developments in the field of information and telecommunications in the context of international security" and Resolution 73/266 "Advancing responsible State behaviour in cyberspace in the context of international security"

REPORT

France welcomes this opportunity to respond to United Nations General Assembly **Resolution 73/27** "Developments in the field of information and telecommunications in the context of international security" and **Resolution 73/266** "Advancing responsible State behaviour in cyberspace in the context of international security".

1. Overall assessment of cyber security issues

Firstly, France would like to recall that it does not employ the term "information security" but rather the term "information systems security" or "cyber security". Active in the promotion of freedom of expression online (2018 Human Rights Council Resolution A/HRC/38/L.10/Rev.1), **France does not consider that information as such can be a factor of vulnerability** against which it is necessary to protect oneself, without prejudice to measures that could be taken proportionately, transparently and under the conditions strictly established by law under Article 19 of the International Covenant on Civil and Political Rights.

The term "cyber security" is more precise in that it designates the resistance of a system to events from cyber space that could compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cyber security makes use of information systems security techniques and is based on fighting cybercrime and implementing cyber defence.

France considers that the cyber space should remain a space of freedom, exchange and growth and is necessary for the prosperity and progress of our societies. As it already highlighted in its National Digital Security Strategy[1] in 2015, France considers that "providing new uses and new services, digital technology is a factor of innovation. It generates change in most professions. It transforms the sectors of activities and enterprises to make them more flexible and competitive." It provides opportunities for companies to improve their daily operations through online communication, commerce, information and economic services with a focus on competition and the collaborative economy.

[1] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

This open, secure, stable, accessible and peaceful cyber space, which provides economic, political and social opportunities and has been promoted by France for three decades, is today threatened by new destructive practices developing in cyber space. Specific features of the cyber space (relative anonymity, low costs and easy access to malicious tools, easy implementation, growing vulnerabilities, etc.) enable a number of actors to develop digital arsenals for **spying**, **illicit trafficking**, **destabilization** and **sabotage**. Although certain low-level threats do not fall within the realm of national security but are rather a form of crime, the use of these **cyber weapons** targeting government information systems, critical infrastructure and large companies can have serious consequences.

Cyber security issues are now an integral part of power strategies and relationships that govern international relations. Cyber security is therefore a top priority and political issue. As the **2017 Strategic Review of Defence and National Security**[2] highlights, "the massive digital transformation that has been taking place in our societies over the past decade, combined with globally interconnected information and communication systems, is prompting the emergence of new threats as well as new opportunities. These developments provide universal access to powerful tools for self-expression, influence, propaganda and intelligence, making available not only huge volumes of data but also formidable means of attack. They have facilitated the rise of new private actors that are able to assert their presence on the international stage, as challenges to state sovereignty as well as essential partners in some cases. As a result, they are reshaping the balance of power between state, non-state, and private-sector actors."

We all share the responsibility to preserve, develop and promote a cyber space that is open, stable, accessible and peaceful. In the face of common threats to stability and international security, for several years, France has implemented an active diplomacy and policy to strengthen security, trust and stability in cyber space.

2. Efforts to strengthen cyber security at national level and promote international cooperation in this area.

a. Strengthening France's cyber security apparatus

The strategic guidance adopted in recent years at the highest government level continue to include cyber security as a priority of the government's action.

France is scaling up its national apparatus. For the past ten years, France has taken measures including the creation and development of the French National Cyber Security Agency (ANSSI) in 2009, the drafting of the first French strategy for the defence and security of information systems in February 2011, the strengthening of legal tools and the substantial increase in resources devoted to cyber security in the most recent military programming law, the publication of the Cyber Defence Pact in February 2014 by the Ministry for the Armed

[2] https://www.defense.gouv.fr/dgris/presentation/evenements-archives/revue-strategique-de-defense-et-de-securite-nationale-2017

Forces and the creation of a Cyber Defence Centre of Excellence aiming to develop training, academic research and the industrial and technological base in the area of cyber security. France has also implemented a national and international policy of **transparency** regarding its strategy.

In 2015, France developed a National Digital Security Strategy[3] to support the digital transition of French society. It emphasizes a strong response to malicious cyber activities and aims to make cyber security a competitive advantage for French companies.

In December 2017, France's International Digital Strategy[4] **supplemented this document** setting out the principles and objectives that France is pursuing internationally in cyber space. Based on three key pillars (governance, the economy and security), this strategy focuses on:

- Promoting an open, diverse and trustworthy digital space at a global level;
- Fostering a European model, striking a balance between economic growth, basic rights and security;
- Strengthening the influence, attractiveness, security and trade stances of France and French actors in cyber space.

The Strategic Review of Cyber Defence[5] **presented in February 2018 defines a cyber crisis management doctrine and sets out detailed national strategic cyber defence objectives**. Confirming the relevance of the French model and government's foremost responsibility for cyber security, it is based on seven main principles:

- Improving the protection of our country's information systems;
- Deterring attacks through a set of defensive measures involving strengthened resilience as well as reaction and response capabilities;
- Affirming and exercising French digital sovereignty;
- Providing a more effective penal response to cybercrime;
- Promoting a shared information security culture;
- Participating in the development of a digital Europe that is secure and trustworthy;
- Taking international action to promote a collective and well-ordered cyber space governance.

The 2019-2025 military programming law[6]**, building on previous programming acts, provides for a substantial increase in resources allocated to cyber defence**, particularly in the area of personnel, with an aim of recruiting 1,500 additional people to increase the number of personnel working on these issues to 4,000 at the Ministry for the Armed Forces by 2025.

The following actors contribute to the effectiveness of the technical and operational apparatus:

- **The French National Cyber Security Agency** (ANSSI) is responsible for preventing (including through normative means) and reacting effectively to IT incidents targeting

[3] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[4] https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf
[5] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf
[6] https://www.legifrance.gouv.fr/eli/loi/2018/7/13/ARMX1800503L/jo/texte

government and operators of vital importance (critical national infrastructure). Today it employs 600 people and continues to grow. It has become a leader in the definition of pertinent cyber security norms.

- **The Ministry for the Armed Force**s has a dual mission to protect the networks required for its action and to make operations in cyber space a focus of military action. In order to consolidate the Ministry's action in this area, a **general officer was appointed as cyber defence commander** (COMCYBER) in September 2017. He operates under the orders of the Armed Forces Chief of Staff. In early 2019, the Ministry of Armed Forces published a cyber defensive policy. At the same time, a first public expression of offensive cyber warfare doctrine for military operations was presented by the Armed Forces Chief of Staff.

- The role of the **Ministry of the Interior** and the **Ministry of Justice** is to combat all forms of cybercrime, targeting national institutions and interests, economic actors and government authorities, and individuals.

b. Promoting international cooperation for the stability and security of cyber space

Strengthening strategic stability and international security in cyber space is one of France's priorities. According to the Strategic Review of Cyber Defence, "improving cooperation within the international community in cyber space is an effective way to increase stability, through greater mutual knowledge and even trust between actors, as well as establishing mechanisms for joint crisis management, communication and de-escalation." France's actions to promote international cooperation on cyber security issues are conducted both at the European and the international level.

- *Preventing crises by strengthening cooperation and building capability*

France considers that the main objective pursued by its policy in the digital space is preventing crises. As the Strategic Review of Cyber Defence highlights, "the strengthening of protection, resilience and cooperation of all cyber space actors directly strengthens our national security." If this aim is to be achieved, technical, operational and structural cooperation with government partners and international organizations needs to be enhanced with a view to developing the capabilities of these various actors and the overall resilience of cyber space.

As networks and societies are very interconnected, France considers that the cyber security of all can only be ensured when every State has sufficient capabilities to secure its own information systems. That is why it has worked to build the cyber security capabilities of its partners bilaterally and within the framework of multilateral initiatives. This

investment in cooperation benefits all parties. It allows France to remain on the cutting edge by interacting with its peers and learning from them. As a result, all parties gain knowledge and expertise and build mutual trust.

At the technical level, ANSSI is establishing partnerships with its counterparts from many countries to promote the sharing of essential data, such as information concerning vulnerabilities or flaws in products or services. The Computer Emergency Response Team – France (CERT-FR) working within ANSSI is part of **several multilateral networks** (FIRST, TF-CSIRT, EGC, European Union CSIRTs Network) through which it maintains contacts with CERTs worldwide.

France is implementing a pro-active policy of operational and structural cooperation. In recent years, France has sent international cyber security experts to work with internal security forces of partner countries. With Senegal, France is also launching activities at the Cybersecurity School in Dakar inaugurated at the end of 2018, which is a national school with a regional reach. A priority of this project is to provide short and adaptable training courses for cyber security professionals and senior officials from West Africa as a priority.

With the aim of strengthening cyber resilience in the European Union, France is helping to develop a voluntary cooperation framework to prevent and resolve incidents. It is based on the development of common operational standards and procedures for cooperation among partners, which have been tested during pan-European exercises. France has also helped draft a "**cyber toolbox"** providing a European framework for a joint diplomatic response to cyber-attacks through the use of prevention, cooperation and stabilization measures.

France has also worked for the adoption of a European regulation taking into account competition demands and digital technology potential while protecting its citizens, companies and Member States (right to privacy and personal data protection, protection of critical infrastructure, fight against online terrorist content). This can be seen in the adoption of **Regulation (EU) 2016/679 on the protection of data (GDPR)** and **Directive (EU) 2016/1146 on the security of network and information systems (NIS Directive)** as well as the upcoming entry into force of the regulation regarding the European Union Agency for Network and Information Security (ENISA), through the certification of the cyber security of information and communication technologies and the repealing of Regulation (EU) No. 526/2013 on cyber security. France also actively supports the adoption of a European regulation aiming to prevent the dissemination of terrorist content online and to impose uniform obligations on Internet operators. Lastly, France is working for the **European Union's industrial policy** to support high-tech research and development capabilities to foster the deployment of reliable and evaluated cyber security technology services.

Within NATO, France was a driver in the adoption of the Allies' **Cyber Defence Pledge** at the Warsaw Summit in June 2016. This pledge ensures that each NATO Member States dedicates an appropriate portion of its resources to building its cyber defence capabilities, thereby increasing everyone's overall level of security. In May 2018, France hosted the first Cyber Defence Pledge Conference. Furthermore, the Allies recognized cyberspace as a field

of operations, thereby committing NATO to defend itself there as it does on land, in the air and at sea.

- *Preventing crises by developing norms regulating the behaviour of actors in cyber space*

France considers that the emergence of a collective cyber security framework can only be based on balances defined by international law. France's International Digital Strategy underlines how important it is for France to pursue "cooperative dialogue with all private and public actors concerned, and all international partners willing to do so bilaterally and multilaterally".

France took an active part in United Nations negotiations conducted in the framework of the last five round of the Group of Governmental Experts on cyber security. **It will pursue its commitment in the resuming discussions** both in the Group of Governmental Experts as well as in the Open-Ended Working Group to promote its vision of a cyber space of freedom, exchange and growth, which is necessary for the prosperity and progress of our societies. It is also involved in other international fora where these cyber security issues are addressed.

France ratified the **Budapest Convention on Cybercrime in 2006,** which provides a legal basis for establishing the different cybercrime offences and provides for flexible and modern means for international cooperation in this area (for example, a 24/7 network to accelerate procedures for assistance among States Parties). France advocates the **universalization of the Budapest Convention** which now has **63 States Parties from every continent**. It **actively participates in the negotiation of its second additional protocol** which aims to enhance international cooperation in this area by developing law enforcement cooperation and mutual legal assistance, particularly when it comes to access to electronic evidence. France also supports the **work of the open-ended Intergovernmental Expert Group** to conduct an in-depth study of the problem of cybercrime which confirms the central role of the UNODC in this area.

Presented by the President of the French Republic at the Internet Governance Forum held at UNESCO on 12 November 2018, the **Paris Call for Trust and Security in Cyberspace**[7] is evidence of the active role France plays in promoting a secure, stable and open cyber space. Supported today by 66 countries and nearly 500 non-state entities, this text aims to promote certain fundamental principles of the regulation of cyber space including the implementation of international law and human rights in cyber space, responsible behaviour of States, state monopoly of legitimate violence, the recognition of specific responsibilities of private actors, etc.

France has also taken action within the **Organization for Economic Co-operation and Development.** It helped organize the first meeting of the "OECD Global Forum on Digital

[7] https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf

Security for Prosperity" in December 2018, on the theme of **the responsibility of private actors** in digital security.

At the G7, the Ise-Shima Cyber Group, which was created in 2016, led to the adoption in 2017 of an ambitious declaration, known as the **Lucca Declaration** on Responsible State Behavior in Cyberspace. In March 2019, as part of its G7 Presidency, France proposed launching a **follow-up mechanism on the implementation of the norms and recommendations approved at UN level**, endorsed by the Dinard Declaration on the Cyber Norm Initiative.[8]

Within the G20, France is working so that the G20 focuses on fundamental issues of competition in the digital economy and new methods of regulation and governance such as digital security, in the same vein as the "Paris Call".

France, which is actively involved in the **Organization for Security and Co-operation in Europe's** Informal Working Group on ICT Security, continues to promote the operationalization of the 16 confidence-building measures (CBMs) developed by the OSCE on cyber issues. Among other things, it is leading the implementation of a confidence-building measure on securing critical infrastructures (CBM 15).

With a view to intensifying the fight against the proliferation of malicious tools and techniques, France supported the addition of intrusion software into the control list of the Wassenaar Arrangement (WA). France believes that regulation efforts must continue to that end by listing some types of softwares as weapons, due to the gravity of the effects they could cause.

France believes that many cyber security-linked issues deserve a multi-stakeholder approach, in order to take account of the role and specific responsibilities of non-state actors. In line with this, France supported the activities of the **Global Commission on the Stability of Cyberspace** (GCSC). This Commission aims to develop proposals for norms and policies to enhance international security and stability and guide responsible state behaviour in cyber space.

3. Relevant international concepts to strengthen overall cyber security

a. Concepts to maintain international peace and security

In order to ensure an open, safe, stable, accessible and peaceful cyber space, France reiterates its commitment to the applicability of international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law, to the use of information and communication technology (ICT) by States.

- International public law

[8] https://www.elysee.fr/admin/upload/default/0001/04/d37b5326306c7513b58c79d26938f678d95cb2ff.pdf

As the United Nations Group of Governmental Experts (GGE) concluded in its report published in 2013, the principles and rules of international law apply to the behaviour of States in cyber space. While cyber space has its own specific features (anonymity, role of private stakeholders, etc.), international law nonetheless provides the means to responsibly govern States' behaviour in this environment. In this regard, the inability to attribute responsibility is not a definitive obstacle to the application of existing international law.

The principle of sovereignty applies to cyber space. To this end, France reaffirms that it is exercising its sovereignty over information systems, persons and cyber activities in its territory, within the bounds of its obligations stemming from international law. The unauthorized penetration of French systems or the production of effects in French territory via cyber means by a State entity, or non-state actors acting under the instructions or the control of a State, can constitute a violation of sovereignty.

The range of measures that States can adopt in response to a cyber-attack depends on its gravity. The more serious the attack, the broader the range of measures. A cyber operation can be deemed to be a use of force as prohibited under Article 2.4 of the Charter of the United Nations. Crossing the threshold of the use of force is not based on the cyber resources used, but on the effects of the cyber operation. If these effects are similar to those produced by conventional weapons, the cyber operation can be deemed to be a use of force. France believes that if the scale or effects of a major cyber-attack, perpetrated by a State or non-state actors acting under the control or instructions of a State, were to reach a sufficient gravity threshold (e.g. substantial loss of human life, significant physical damage, damage to critical infrastructures with significant consequences), and were to be attributable to a State, it could be deemed an "armed attack" under Article 51 of the Charter of the United Nations, thus justifying the invocation of self-defence. This self-defence can be implemented through conventional or cyber means provided that the principles of necessity and proportionality are observed. Classifying a cyber-attack as an "armed attack" under Article 51 of the Charter of the United Nations is a political decision taken on a case-by-case basis based on the criteria set out by international law.

France does not believe it currently necessary to create a new legally-binding international instrument specifically for cyber security issues. In cyber space, like in other areas, existing international law is applicable and must be observed.

- International humanitarian law (IHL)

France supports the applicability of international humanitarian law in cyber operations carried out as part of and in connection with armed conflicts.

Currently, offensive cyber warfare operations support conventional military operations. The idea of an armed conflict exclusively comprised of cyber activities cannot be ruled out in principle, but rests on the ability of cyber operations to reach the threshold of violence required to constitute an international or non-international armed conflict.

Despite the fact that they are digitalized, these operations remain subject to the geographical scope of IHL, i.e. their effects are restricted to the territory of the States Parties in international armed conflict or the territory in which the hostilities are taking place as part of a non-international armed conflict.

Offensive cyber warfare operations implemented by the French armed forces are subject to IHL principles, including:

- the **principle of distinction** between civilian objects and military objectives. To this end, cyber-attacks which are not directed at a specific military objective or which are implemented using cyber weapons which cannot be directed at a specific military objective are prohibited. In this respect, certain content data, while intangible, can be deemed to be protected civilian objects under IHL.

- the **principle of humanity**. They must not target the civilian population as such or individual civilians, unless they are taking a direct part in hostilities and during this participation. In the context of armed conflict, any cyber combatant who is a member of the armed forces, any member of an organized armed group committing cyber-attacks against an opposing party, or any civilian taking a direct part in hostilities via cyber resources can be subject to an attack by cyber or conventional means;

- the **principle of proportionality** Civilians and civilian objects must be protected constantly from the effects of hostilities while there are cyber warfare operations. Collateral damage cannot exceed the expected direct and concrete military advantage. Respect for the principle of proportionality in cyber space requires taking account of all predictable effects of the weapon, whether they be direct (damage to the targeted system, service suspended, etc.) or indirect (effects on the infrastructure controlled by the attacked system, but also on the people affected by the malfunctioning or destruction of systems or by the alteration and corruption of the content data) as long as they have a sufficient causal link with the attack. This principle also prohibits the use of cyber weapons which cannot be controlled (especially in time and space), in other words which can cause irreversible damage to civilian infrastructure, systems or data.

These points are recalled in the public components of French military doctrine on offensive cyber warfare which were set out in early 2019.

- Human rights

France believes that the rights people enjoy offline must also be protected online, and that international human rights law applies to cyber space. These values are in particular undermined by the spread of illegal content (terrorism, hate speech, anti-Semitism). France believes it particularly necessary to involve the private digital stakeholders in the fight against illegal content and to clarify their role and responsibilities internationally to combat this illegal content and guarantee the protection of human rights and fundamental freedoms online.

- Principle of due diligence

France believes it essential to reach a shared understanding at international level of the obligations on States of which the infrastructure is believed to be being used for malicious purposes, against the interests of another State. The aim is to clarify the application, in cyber space, of the **principle of due diligence**, which states that it is "every State's obligation not to knowingly allow its territory to be used for acts contrary to the rights of other States".[9] To this end, States must not knowingly allow their territory to be used to commit internationally illegal acts through cyber means and not use non-state intermediaries (proxies) to violate international law. A better understanding of how to apply this principle to cyber issues would help bolster cooperation between States with a view to protecting certain critical infrastructure but also to put a stop to major cyber-attacks perpetrated via a third State.

b. Concept helping to strengthen cooperation and confidence among States

- Norms of behaviour

The various negotiating cycles carried out as part of the UN GGE on cyber security have enabled significant progress to be made as regards the international regulation of cyber space. The 2015 report identifies 11 norms of responsible state behaviour in cyber space. France believes that each State must observe these norms and develop mechanisms to implement them. Other norms, which are applicable to the behaviour of States or that of other actors in cyber space, could also be developed in the future.

- Confidence-building measures

The work carried out in various regional fora and organizations with a view to developing confidence-building measures specific to cyber security issues must be intensified. France continues to encourage its partners to create interministerial procedures which can be used in order to ensure good communication between States during crises. Developing such procedures and mechanisms, based on transparency and communication, is essential to preventing conflicts in cyber space.

- Capacity building

France supports the goal of international capacity-building in the area of cyber security. Such efforts directly help to increase everyone's security and the stability of cyber space. France intends to play a full role in these efforts through bilateral, regional and multilateral capacity-building actions.

[9] *The Corfu Channel Case*, Judgment of 9 April 1949: I.C.J., Reports 1949, p. 4

c. Role and responsibility of non-state actors

- Multi-stakeholder approach

In the "Paris Call", France highlighted the "necessity of a strengthened multi-stakeholder approach". France believes that civil society, academia, the private sector and the technical community have skills and resources which are useful in defining certain aspects of relevant cyber security policies.

- Security responsibility of private stakeholders in designing and maintaining digital products

The huge growth in digital technology as a new tool and space for confrontation gives the private sector, and in particular a number of systemic actors, a critical role and an unprecedented responsibility in maintaining international peace and security. The Paris Call recognizes the "responsibilities of key private sector actors in improving trust, security and stability in cyberspace" and encourages "initiatives aimed at strengthening the security of digital processes, products and services."

France believes that it is relevant to set out at the international level a principle of security responsibility for systemic private actors in the design, integration, deployment and maintenance of their products, processes and digital services, throughout their life cycle and from one end of the supply chain to the other.

- Responsibility of digital platforms in counter-terrorism

France is also working to make private digital technology actors accountable in combating the misuse of their services for terrorist purposes. It is acting in particular within the **G7** and the **EU**, where it is actively supporting a **proposed European regulation** to govern the action of Internet operators on fighting terrorist content online. This text requires that terrorist content be removed within one hour at the request of a Member State, that proactive measures be taken for platforms exposed to terrorist content, that a permanently-available point of contact be established to process referrals and withdrawal requests, and that sanctions be imposed in the event of persistent failure to cooperate.

- Preventing offensive activities by private actors

France believes that States must maintain their monopoly on legitimate physical violence, in both cyber space and other areas. To this end, it supports the ban on non-state actors, including from the private sector, conducting offensive activities in cyber space on their own behalf and that of other non-state actors. These practices, which are based on the principle of private self-defence (*hack-back*) are potentially destabilizing due to their negative consequences on third parties and could fuel an escalation in tensions between States. To this end, France believes it necessary to clarify the leeway afforded to private actors as regards how they respond to incidents.

4. Measures available to the international community to enhance cyber security across the board

In the face of the new threats of the digital revolution, France believes that cooperation and law are required to prevent cyber space from becoming a permanent conflict zone. Like in other areas, States must comply with international law in cyber space. Furthermore, a body of norms governing the responsible behaviour of States in cyber space has emerged in recent years, which must be consolidated. France believes that the following measures could be taken to strengthen cyber space internationally:

- **Build on the work of the previous GGEs**: without undermining the norms and recommendations on which there was consensus during the previous negotiating cycles, it could be useful to specify how these norms and recommendations can be implemented and to develop a better international understanding of best practices in the area;

- **Draw on the "Paris Call for Trust and Security in Cyberspace" during the upcoming discussions on cyber security issues at the UN**: that declaration currently has the support of over one third of United Nations Member States, and several hundred leading non-state actors, with a shared vision of the principles on which the behaviour of the various actors in cyber space should be based.

- **Universalize the Budapest Convention on Cybercrime**: adopted in November 2001 to step up international cooperation in the area, this instrument has now been ratified by 63 States and has influenced the national legislation of over two thirds of United Nations Member States;

- **Encourage States to be transparent**: especially as regards their cyber security strategy, their doctrine for managing cyber crises and responding to a cyber-attack and their interpretation of how international law applies in cyber space;

- **Operationalize the confidence-building measures specific to cyber issues which have been developed, within regional or international frameworks**;

- **Step up initiatives and mechanisms enabling the exchange of best practices and capacity building**: such mechanisms should aim to provide all States with an effective cyber security mechanism, in particular one involving:

    - Setting up a cyber security strategy;
    - Defining a legislative framework to promote cyber security and the fight against cybercrime;
    - Creating a Computer Emergency Response Team (CERT);

- Setting up procedures for cooperating with the private sector, including major tech companies;
- Defining a framework for protecting critical infrastructure in cyber space.

- **Recognize on an international scale a principle of security responsibility for systemic private actors** in the design, integration, deployment and maintenance of their products, processes and digital services, throughout their life cycle and from one end of the supply chain to the other.