United Nations S/PV.7882

Security Council

Seventy-second year

Provisional

7882nd meeting

Monday, 13 February 2017, 10 a.m.

New York

President:	Mr. Klimkin/Mr. Vitrenko	(Ukraine)
Members:	Bolivia (Plurinational State of)	Mr. Arancibia Fernández
	China	Mr. Liu Jieyi
	Egypt	Mr. Aboulatta
	Ethiopia	Mr. Alemu
	France	Mr. Lamek
	Italy	Mr. Amendola
	Japan	Mr. Bessho
	Kazakhstan	Mr. Abdymomunov
	Russian Federation	Mr. Zagaynov
	Senegal	Mr. Seck
	Sweden	Mr. Skoog
	United Kingdom of Great Britain and Northern Ireland	Mr. Rycroft
	United States of America	Mr. Klein
	Uruguay	Mr. Bermúdez

Agenda

Threats to international peace and security caused by terrorist acts

Protection of critical infrastructure against terrorist attacks

Letter dated 1 February 2017 from the Permanent Representative of Ukraine to the United Nations addressed to the Secretary-General (S/2017/104)

17-03821 (E)

The meeting was called to order at 10.10 a.m.

Adoption of the agenda

The agenda was adopted.

Threats to international peace and security caused by terrorist acts

Protection of critical infrastructure against terrorist attacks

Letter dated 1 February 2017 from the Permanent Representative of Ukraine to the United Nations addressed to the Secretary-General (S/2017/104)

The President: In accordance with rule 37 of the Council's provisional rules of procedure, I invite the representatives of Afghanistan, Albania, Algeria, Argentina, Australia, Austria, Bangladesh, Belgium, Brazil, Bulgaria, Canada, Chile, Colombia, Croatia, Cuba, the Czech Republic, Denmark, Estonia, Finland, Georgia, Germany, Greece, Haiti, Iceland, India, Indonesia, Iraq, the Islamic Republic of Iran, Israel, Jordan, Kuwait, Latvia, Luxembourg, Malaysia, Maldives, Malta, Montenegro, Morocco, the Netherlands, New Zealand, Pakistan, Peru, Poland, the Republic of Korea, the Republic of Moldova, Romania, Slovakia, Slovenia, South Africa, Spain, the Syrian Arab Republic, the former Yugoslav Republic of Macedonia, Turkey, the United Arab Emirates and the Bolivarian Republic of Venezuela to participate in this meeting.

In accordance with rule 39 of the Council's provisional rules of procedure, I invite the following briefers to participate in this meeting: Ms. Maria Luiza Ribeiro Viotti, Chef de Cabinet of the Secretary-General; Mr. Jürgen Stock, Secretary General of the International Criminal Police Organization; Mr. Hamid Ali Rao, Deputy Director-General of the Organization for the Prohibition of Chemical Weapons; Mr. Chris Trelawny, Special Adviser to the Secretary-General of the International Maritime Organization on Maritime Security and Facilitation; and Mr. Olli Heinonen, Senior Advisor on Science and Non-proliferation at the Foundation for Defense of Democracies and former Deputy Director General of the International Atomic Energy Agency.

Mr. Stock is joining today's meeting via video teleconference from Lyon.

In accordance with rule 39 of the Council's provisional rules of procedure, I also invite the following persons to participate in this meeting: Mr. João Vale de Almeida, Head of the Delegation of the European Union to the United Nations; and Mr. Krisztian Meszaros, Civilian Liaison Officer of the North Atlantic Treaty Organization to the United Nations.

I propose that the Council invite the Permanent Observer of the Observer State of the Holy See to the United Nations to participate in the meeting, in accordance with the provisional rules of procedure and the previous practice in this regard.

There being no objection, it is so decided.

The Security Council will now begin its consideration of the item on its agenda.

I wish to draw the attention of Council members to document S/2017/104, which contains the text of a letter dated 1 February 2017 from the Permanent Representative of Ukraine to the United Nations addressed to the Secretary-General, transmitting a concept note on the item under consideration.

Members of the Council have before them document S/2017/119, which contains the text of a draft resolution submitted by Albania, Austria, Belgium, Bulgaria, Canada, Chile, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Iceland, Iraq, Israel, Italy, Japan, Latvia, Luxembourg, Malaysia, Malta, Montenegro, the Netherlands, New Zealand, Poland, the Republic of Moldova, Romania, Slovakia, Slovenia, Spain, Sweden, the former Yugoslav Republic of Macedonia, Turkey, Ukraine, the United Arab Emirates, the United Kingdom of Great Britain and Northern Ireland, the United States of America and Uruguay.

The Council is ready to proceed to the vote on the draft resolution before it. I shall put the draft resolution to the vote now.

A vote was taken by show of hands.

In favour:

Bolivia (Plurinational State of), China, Egypt, Ethiopia, France, Italy, Japan, Kazakhstan, Russian Federation, Senegal, Sweden, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America and Uruguay

The President: The draft resolution received 15 votes in favour. The draft resolution has been adopted unanimously as resolution 2341 (2017).

On 21 November 2016, the Security Council held an Arria Formula meeting on the protection of critical infrastructure against terrorist attacks. This meeting demonstrated a growing understanding among States Members of the United Nations of the importance of the subject and attested to an urgent need to ensure a high level of protection of critical infrastructure and to consolidate international efforts in increasing resilience against terrorist attacks. In our view, the resolution just adopted is a timely response by the international community to emerging and rapidly evolving threats posed by terrorism. This is a decisive step towards global preparedness for terrorist attacks against critical infrastructure and the strengthening of international cooperation on this matter. I encourage participants in today's debate to discuss in detail their priorities and challenges, to provide information on their current efforts and to share good practices in the area of protection of critical infrastructure.

I now give the floor to Ms. Viotti.

Ms. Viotti: It is a pleasure for me to be here today on behalf of the Secretary-General. I would like to congratulate you, Sir, on convening this meeting.

As terrorist organizations proliferate and seek innovative ways to plan and execute physical and cyberattacks across the globe, the threat they pose is becoming increasingly complex. Critical infrastructure is especially vulnerable, including energy facilities and networks; air, land and maritime transportation; banking and financial services; water supply; food distribution, public health and other services that are the backbone of modern societies. Infrastructure networks and systems that previously functioned independently have become interlinked through advances in communication and information technology. An attack on one sector can affect others, leading to disruptions and widespread chaos.

The Counter-Terrorism Committee Executive Directorate has recognized the gravity of the dangers of Da'esh and other groups determined to carry out such attacks. Moreover, since many such facilities and networks operate across borders, any terrorist attack against them would almost certainly have regional and global implications. The transnational nature of terrorism requires the coordinated response on the part of all States and actors of the international community.

However, we need to admit that international counter-terrorism cooperation has been limited, especially in the area of critical infrastructure. Strategically, this means that the international community needs to unite and be more creative, proactive and effective, including through the development of strong public-private partnerships. Three key steps need to be taken.

First, vulnerabilities in critical infrastructure need to be mapped at all levels and in all sectors. Secondly, international, regional and national actors should cooperate on prevention and, in case an attack does take place, on the mitigation of its effects, including through information-sharing. Thirdly, it is crucial to build States' capacities, including to assess risks, take preparedness measures, strengthen emergency management capacity and ensure that responses are fully in keeping with human rights norms and standards. The United Nations stands ready to assist Member States in these and other areas.

The Counter-Terrorism Implementation Task Force has set up the Inter-agency Working Group on the Protection of Critical Infrastructure including Internet, Vulnerable Targets and Tourism Security. Various projects to assist Member States are under way, encompassing many areas, United Nations entities and partners. But of course, the primary responsibility lies with Member States.

This debate comes at a crucial time. As our world becomes increasingly interconnected through travel, commerce and communications and in cyberspace, we become more vulnerable to attacks by technologically savvy terrorists seeking new ways to spread fear. It is encouraging that the Security Council has heightened its attention to this critical threat.

The President: I thank Ms. Viotti for her briefing.

I now give the floor to Mr. Stock.

Mr. Stock: It is an honour to brief the Security Council once again, and on an issue of central importance to our collective security.

I would like to thank Ukraine for convening this meeting and for its continued efforts to mobilize international cooperation on this crucial subject.

Critical infrastructure acts as the life-support system of our everyday existence. Our societies are

sustained by a highly complex and sophisticated network of infrastructure systems. Our citizens expect and rely upon functioning institutions and services for their health, safety, security and economic well-being. This life-support system has become more efficient and productive due to technological advances, the interchanges of globalization and the demands of an increasingly urban population. The advent of life 3.0 — the overlapping of the digital and physical worlds — allowed us to monitor and even control infrastructure from anywhere in the world.

However, with heavy reliance and real-time connectivity comes vulnerability to threats. The interdependence of our infrastructure through sectors and industries, between the cyber and physical areas, and across national boundaries means that the consequences of an attack could be far-reaching. One attack on a single point of failure could lead to the disruption or destruction of multiple vital systems in the country directly affected, and a ripple effect worldwide. This creates an appealing target to those intending to harm us, and as our cities and infrastructure evolve, so do their weapons. Conflict zone tactics — such as simultaneous active shooter events, armoured vehicle-borne improvised explosive devices, homemade explosive vests, hacking attacks or portable unmanned aerial systems with explosive payloads — could be honed for use in our city streets and against key facilities.

So how can we protect the vital organs of our life-support system against this ever-adapting threat? The short answer is that we can do so by getting all relevant actors able to prepare, prevent and respond to such attacks. These imperatives are at the core of the efforts of INTERPOL and our partners in the Working Group on the Protection of Critical Infrastructure including Internet, Vulnerable Targets and Tourism Security of the Counter-Terrorism Implementation Task Force to promote intelligence-sharing, capacity-building and resilience in some crucial areas.

First, we focus on strengthening critical site security with emergency-preparedness standards and procedures. For instance, INTERPOL's Vulnerable Targets Team has been working with our member countries in West Africa to enhance the physical security of laboratories hosting dangerous pathogens and to protect them from terrorist attacks. Generously funded by the Canadian Government, this project seeks to build biosecurity action plans through joint inter-agency action.

Secondly, we continue to urge countries to protect their borders and counter terrorist mobility. As mentioned in the Secretary-General's report on the threat posed by the Islamic State in Iraq and the Levant (S/2017/97), discussed here last week (see S/PV.7877), between October 2016 and January 2017 INTERPOL observed a 63 per cent increase in the number of profiles of foreign terrorist fighters accessible in real time through its criminal information system, and a 750 per cent increase in the sharing of information by member countries through its channels. This is simply unprecedented in such a sensitive area; the call issued by the Security Council created a watershed.

Thirdly, it is essential to remain vigilant and increase efforts to interdict materials and tools before they become the next weapon. In this context, INTERPOL works closely with the International Atomic Energy Agency on mitigating the illicit trafficking of radiological and nuclear materials through training in monitoring and detection, and cross-border operations.

Lastly and above all, INTERPOL encourages inter-agency and international collaboration as a force multiplier. The exchange of information, urgent threats detected and best practices in identifying vulnerabilities, methodologies and lessons learned is crucial.

In law enforcement, we are keenly aware of the tragic paradox that a terrorist incident is often an opportunity for learning and improving. Sharing these lessons across borders means reaping the benefits without paying that cost. It is a win-win scenario. Together we can build a global infrastructure security toolkit and incident-response mechanisms that are based on real-life operational experience. In parallel, we can test ourselves with plausible scenarios we may have to face in future.

To that end, INTERPOL organizes events for experts from all involved stakeholders. Our joint symposium, hosted by the United States Federal Bureau of Investigation, is a case in point. Our recent digital security challenge, together with private-sector specialists, is another example of how we are working with member countries and donors to prepare, prevent and respond to threats, be they physical, digital or both.

In an interconnected world, we will not succeed in protecting national infrastructures in isolation. That is why initiatives such as this meeting and the steps that will be taken as a result by the international community are essential.

The President: I thank Mr. Stock for his briefing.

I now give the floor to Mr. Rao.

Mr. Rao: Allow me to begin, Sir, by offering you my congratulations on your assumption of the presidency of the Security Council. On behalf of the Director-General of the Organization for the Prohibition of Chemical Weapons (OPCW), I wish to thank you for having invited the OPCW to brief on this important issue.

This year the OPCW is celebrating 20 years of working together for a world free of chemical weapons. As we remain on track to eliminate and verify all chemical weapons declared by possessor States by the early part of the next decade, we are redoubling our efforts to prevent their re-emergence.

The OPCW is not a counter-terrorism organization, but it is a credit to the commitment of our States parties that they have recognized the organization as a forum that can make a meaningful contribution to global counter-terrorism efforts, especially with regard to the threat of chemical terrorism.

Since 2009, the OPCW has been implementing and expanding international cooperation programmes aimed at enhancing global chemical security. At the request of States parties, the OPCW conducts a comprehensive risk assessment to help them determine chemical-security threats. The aim of capacity-building in such countries is to assist in assessing risks, increasing vigilance, instituting protective measures and responding to threats. Capacity-building programmes involve a wide range of stakeholders, including facility managers, police, academics, laboratory staff and chemical, biological, radiological or nuclear experts in order to strengthen the security framework at the country level. Experts from neighbouring countries are included, as appropriate, to increase the footprint of the security framework regionally.

As we strengthen our role as a platform for information-sharing and coordination, we have reinvigorated the work of the Open-Ended Working Group on Terrorism through the creation of a sub-working group on non-State actors. The group addresses the legal, prevention and response aspects of countering chemical terrorism. The OPCW secretariat has also developed its capacity to assist States parties in responding to possible acts of chemical terrorism. A rapid-response and assistance mission has been established at OPCW headquarters to deploy at short notice to any State party affected by a chemical incident involving the alleged use of toxic chemicals by a non-State actor. The mission will deploy only at the request of the State party affected. The team will be equipped to secure the affected area, detect toxic chemicals and provide advice on decontamination and immediate assistance to victims. Essentially, the team will be equipped to cooperate and coordinate with the United Nations and other relevant international organizations. In January, the mission was tested at a tabletop exercise held in parallel with a United Nations Counter-Terrorism Implementation Task Force meeting at OPCW headquarters.

Secondly, we are working with the chemical industry. Hundreds of thousands of tons of scheduled chemicals are traded internationally every year. As the global chemical industry continues to grow in size and complexity, ensuring that chemicals are never traded, whether knowingly or not, for purposes banned by the Chemical Weapons Convention is a high priority. Security along the chemical-supply chain will play a critical role in protecting people and the environment from the hostile use of toxic chemicals.

We have seen the enormous human and environmental costs that chemical accidents can have. The potential damage is only multiplied if such events are purposely caused by those wishing to do harm. The recent attack on a chemical plant near Mosul, Iraq, illustrates all too vividly the risks we face if those who wish to harm and terrorize focus their sights on the chemical infrastructure. Equal responsibility must be shared between industry and government if we are to raise the chemical-security bar against terrorist attacks. The chemical industry worldwide fully understands the importance of preventing any misuse of chemicals as well as the physical protection of chemical plants, and our close collaboration with the global chemical industry continues to gain in strength.

Thirdly, we are working with our international partners. Combating chemical terrorism requires a broad-ranging approach to security that includes a network of stakeholders and international partners. We engage with major international organizations through

the Counter-Terrorism Implementation Task Force, a body that forms part of the United Nations Global Counter-Terrorism Strategy. The Task Force aims to enhance preparedness and response capacities through a common and coherent framework. As co-Chair of the working group on preventing and responding to weapons of mass destruction attacks, the OPCW has called for enhanced inter-agency coordination in response to a chemical terrorist attack. Last month, the OPCW hosted a tabletop exercise with the working group to clearly outline response capabilities and gaps. The goal of the exercise is to create a comprehensive global response system and to ensure that any country that requests assistance will receive it in a coordinated and effective way.

Also in January, the OPCW signed a memorandum of understanding with the World Customs Organization. Enhanced cooperation with the World Customs Organization is envisaged in order to strengthen national and international controls on the trade of toxic chemicals.

The members of the Council are fully aware of the work that the OPCW carried out jointly with United Nations to eliminate the Syrian Arab Republic's chemical-weapons programme. More than 30 countries committed financial and technical resources to this effort. The private sector played a pivotal role, as chemical funds in multiple countries were also involved in the elimination of some of these agents. Although progress has been made, our work in Syria is not yet complete. It is deeply regrettable that chemical weapons have continued to be used in that country. In Libya, the threat from non-State actors led to a request from the Libyan authorities for assistance in removing and destroying the last remnants of its former chemical-weapons programme. This operation is currently being successfully carried out with the cooperation and support of our States parties.

A world free of chemical weapons can be realized only through a high degree of awareness, a shared vision and the continuing commitment to international cooperation. The Chemical Weapons Convention affirms a common resolve never to allow the science of chemistry to turn against humankind. Through it we will continue to work together with all stakeholders to strengthen the global capacity to prevent and, when needed, to detect and respond to acts of chemical terrorism.

The President: I thank Mr. Rao for his briefing.

I now give the floor to Mr. Trelawny.

Mr. Trelawny: The Secretary-General of the International Maritime Organization (IMO), Mr. Kitack Lim, thanks the President of the Security Council and the Government of Ukraine for the invitation to participate in this high-level open debate on the protection of critical infrastructure against terrorist attacks. He very much regrets that he is unable to be here in person, but has asked me to deliver his statement.

IMO is a specialized agency of the United Nations responsible for the safety, security and efficiency of international maritime transport and the protection of the marine environment. Within the legal framework for the protection of critical infrastructure, IMO is the responsible organization for the Convention on Facilitation of International Maritime Traffic; the International Convention for the Safety of Life at Sea, including the associated International Ship and Port Facility Security Code; and the 1988 and 2005 Conventions for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, and their associated Protocols for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf. Together, these international instruments provide a firm legal basis, both for allowing Parties to bring perpetrators of incidents to justice and for IMO activities in the field of maritime security, including active collaboration with the work of the Security Council's Counter-Terrorism Committee Executive Directorate and the General Assembly's Counter-Terrorism Implementation Task Force.

In the context of security, IMO focuses on what the civil maritime industry — that is, both the shipping and port sectors — and the offshore sector can do to protect themselves and others against possible maritime security threats, including acts of terrorism, and to assist Governments through the implementation of appropriate security measures to protect global maritime trade. The main focus is on preventive security through a continuous risk-management process, which includes procedures for deterrence and threat transfer, rather than countering terrorism per se.

The special measures to enhance maritime security, detailed in chapter XI-2 of the International Convention for the Safety of Life at Sea and the International Ship and Port Facility Security Code, provide a practical, risk-based framework not only for maritime security,

but also for wider application. Although the Convention addresses the safety of life at sea and thereby provides jurisdictional challenges ashore, where most of the preventative security measures are applied, IMO addressed this by leaving it to Member States to define the geographical limits of their port facilities, including their application to offshore installations. IMO also cooperated with the International Labour Organization (ILO) to develop a Code of Practice on Security in Ports, which effectively extended the International Ship and Port Facility Security Code into the wider port area; and with the World Customs Organization on container security, which led to the development and adoption in June 2005 of the SAFE Framework of Standards to Secure and Facilitate Global Trade.

In terms of the practical implementation of chapter X1-2 of the International Convention and the International Ship and Port Facility SecurityCode, it would be fair to say that the main challenges are in the port facilities. Unlike on ships, where an existing safety culture was relatively easy to evolve into a security culture, the security structure in ports is generally far more complex, involving many players from different governmental, law enforcement and private entities. Many countries view ports as critical infrastructure and their security as a facet of national security. However, without clear national and local legislation, policies and direction coordinating the activities of all key stakeholders, security responses in ports are, at best, fragmented.

Critical to the success of port and port facility security regimes, be they for protecting port infrastructure against terrorist attack, countering theft and other criminal activity, or preventing access to ships by terrorists, drug smugglers or stowaways, is a well-coordinated, risk-based preventive strategy. Although IMO has no mandate to assess the compliance of port facilities with chapter X1-2 of the Convention and the International Ship and Port Facility Security Code per se, it is readily apparent that the absence of port and port facility security committees is an indicator of a lack of inter-agency cooperation and thus of poor port facility security. The promotion of such coordination mechanisms, consistent with the ILO/IMO Code of Practice and other guidance issued by IMO, forms the cornerstone of the organization's work on promoting better compliance with chapter X1-2 and the Code.

In fact, since 2001 IMO has developed a range of guidance, self-assessment tools and training materials for the protection of ports, ships and offshore installations. These include model courses for port facility security officers; guidelines on training and certification for port facility security officers; guidance on voluntary self-assessment by Convention Contracting Governments and by port facilities; and consolidated guidance in the form of the Guide to Maritime Security and the Code, published in 2012. IMO has also developed a number of training packages on ship and port security, including the conduct of drills and exercises and the development of maritime security legislation, which are delivered upon request from member Governments. We also have a vibrant programme of technical cooperation activities to assist Member States to develop capacity and capability to deter, prevent, detect and respond to security threats, which complements our 2017 World Maritime Day theme, "IMO: Connecting ships, ports and people".

The world has changed since the introduction of the special measures to enhance maritime security. Ongoing threats to the port, shipping and offshore sectors and related infrastructure continue to evolve. The responses to these challenges have also changed. The Millennium Development Goals for developing countries have been replaced by the Sustainable Development Goals (SDGs) for global application. In this context, IMO actively assists States to address SDG 9 with respect to improving the resilience of infrastructure and other key SDGs. The focus on reactive efforts to counter terrorism have been replaced by a focus on proactive measures to prevent terrorism in the first place.

There is also a need to focus on the opportunities offered by the shipping sector. That involves looking at ports and shipping as wealth-creators within the context of economic development. In this regard, efficient and effective port safety and security is becoming increasingly important and marketable.

One of the biggest challenges to effective implementation of maritime security and maritime law enforcement measures is that they are seen as departmental issues — issues for the navy, coast guard, police, port authority, maritime authority, or customs and border control — with those agencies competing for scarce resources, rather than being part of a national, multi-agency response to developing the port and maritime sector.

Through our programme of capacity-building initiatives to enhance maritime security, IMO's aim is

to work with developed and developing countries, the shipping industry and public and private ports with a view to promoting best practices and building bridges between the diverse actors. At the national level, these include enhancing the efficiency of the whole maritime sector by improving cooperation between ports and ships and developing a closer partnership between the two sectors; raising global standards and setting norms for the safety, security and efficiency of ports and port and coastal State authorities; and improving standardization of port procedures through identifying and developing best practice guidance and training materials.

For the longer- term development of the whole maritime sector, IMO programmes — such as our support to the Yaoundé process in West and Central Africa, pursuant to resolutions 2018 (2011) and 2039 (2012), and the Jeddah Amendment to the Djibouti Code of Conduct 2017, adopted in January — focus on challenging sea-blindness and encouraging investment in the whole of the maritime sector. This includes encouraging national authorities to break down silos and switch from a departmental focus to a national focus and to engage with the private sector. We need not only to encourage the port sector input to national maritime business plans and national and regional maritime and maritime security strategies, but to promote the concept of the port as a service-provider to ships, addressing the us-and-them attitude.

In order to do that, it is vital that national Governments assure their national oversight capability for safety and security and promote the application of the Code and the ILO/IMO Code of Practice in Ports and Offshore Installations. That includes promoting the establishment of port security and facilitation advisory committees as a vehicle for inter-agency cooperation for wider security that addresses all security-related threats, including theft, drugs, illegal wildlife, stowaways, migrant smuggling and terrorism, with Government oversight ensuring effectiveness, an approach that lends itself to the protection of other sectors' critical infrastructure.

Effective security systems require effective procedures, appropriate equipment and, above all, adequately trained and motivated people. At the lowest level, that includes implementing frameworks and developing tools for raising security awareness among all employees. However, in order to ensure the establishment better and more sustainable security systems, Governments and the port sector should develop port security as a career, not just a job, with a focus on developing graduated training packages and programmes aimed at enabling personnel to progress from patrolling and guarding to security supervisory and management roles. There is also significant benefit to be had from developing port-facility security-officer networks designed to help officers exchange best practices and learn from one another.

Although the two modes of transport differ, there are many key similarities between aviation and maritime security, not the least of which are the importance of member States adopting a multi-agency, whole-of-Government approach to the organization of security, including the protection of vital infrastructure; the importance of addressing the whole security system, that is, through threat, risk and vulnerability assessments; the selection, training and certification of personnel; and equipment, procedures and holistic oversight. To those can be added the need for contingency and resilience planning, and for the protection of transport systems and infrastructure to be seen as an enabler of economic development, thus helping to meet sustainable development goals and prevent violent extremism.

As outlined, IMO's maritime security initiatives, conducted in cooperation with the United Nations Office on Drugs and Crime, INTERPOL and others, promote such approaches and, in particular, encourage the establishment of national maritime security and facilitation committees, national security plans and contingency plans endorsed at the highest level, as well as regional communication between national focal points and more comprehensive training and certification programmes for security personnel working at key national points.

The President: I thank Mr. Trelawny for his briefing.

I now give the floor to Mr. Heinonen.

Mr. Heinonen: I appreciate the opportunity to share some of my personal reflections on nuclear terrorism with the Security Council today. I would specifically like to address the issue as it relates to the International Atomic Energy Agency (IAEA) and the Council. To that end, I have given the full version of my statement to the Secretariat, as it includes complementary information supporting some of the points I will make today.

We all understand that a nuclear accident anywhere is a nuclear accident everywhere, as are the ramifications of nuclear terrorism. We are fortunate that so far we have been spared from acts of nuclear terrorism, but we should bear in mind that terrorists have already openly expressed a desire to acquire nuclear weapons. Thefts and other attempts to obtain nuclear and radioactive materials have shown that there are circumstances in which that could happen. Nuclear security can also be compromised in other ways. For instance, the energy industry has been the victim of cyber attacks, including by sabotage at nuclear installations, for which my written statement includes some documentary evidence.

There are two ways in which the risk of nuclear terrorism is heightened today. The first is the increased use and spread of nuclear technology for the production of electricity, radiation technologies in medicine and industry, and the shipment of radioactive and nuclear materials across borders and seas. That brings with it an increase in the number of physical installations and shipments that could be potential targets for terrorist attacks or theft. The second way is a new phenomenon. Terrorist organizations are becoming more sophisticated. A recent report from Conflict Armament Research describing the production by Islamic State in Iraq and the Sham (ISIS) of ammunition reflects a professional approach that included quality controls for the manufacture of its devices. In other words, ISIS is able to attract skilled engineers and other specialists to its production activities, and to internalize sophisticated ways of functioning and means of production. We should therefore not ignore the possibility that such organizations are able to recruit or are at least seeking to co-opt individuals with nuclear skills that could bring insider threats to nuclear installations or increase the probability of the release of dirty bombs, for example.

At the same time, when we are considering the possibility of acts of nuclear terrorism, we should not confine ourselves to traditional ways of thinking about how such acts can occur or be delivered. For instance, just as nuclear material could be used to build dirty bombs, the possession of such toxic materials could also very well be used as for blackmail purposes, or in novel scenarios involving the dissemination of the materials in urban environments. In that regard, we might recall the issue of the possible contamination of water supplies in Damascus in recent weeks. Radioactive materials could be used for similar purposes.

Threats of nuclear terrorism can come from many sources, ranging from sophisticated, well-financed terrorist organizations to nuclear smugglers, hackers capable of launching devastating cyber attacks and individuals with malicious intentions and access to inside information on nuclear installations. We must be prepared to deal with wide-ranging threats from various angles and scenarios. When it comes to operating nuclear installations, all those challenges have an effect on their management by facility operators, regulators and those in charge of emergency planning and response. While every State is responsible for nuclear safety and security on its own territory, we have to be prepared for accidents, emergencies and incidents that have cross-border impact, including handling emergencies arising from the transportation of nuclear and radioactive materials through or near a State's territories. Preparedness and response capabilities should also cover incidents and emergencies arising from possible terrorist acts using materials that do not originate in the target State.

I would like to draw the Council's attention to another sensitive aspect. We should recognize that any assessment of nuclear security relating to the use of nuclear or radioactive materials in military applications in States possessing nuclear weapons remains outside the control of the international community in the situation that exists today.

There are a number of ways that States can approach the issue of better addressing ways to combat nuclear terrorism. They include closer collaboration between nuclear safety and security regimes, as well as changing the roles of the IAEA and the United Nations. While the following list is by no means exhaustive, it should represent good directions to pursue. Safeguards, security and safety are commonly seen as separate areas of nuclear governance. While there are technical and legal reasons justifying that, the three can also coexist and be mutually reinforcing in many ways. They have synergistic effects on one another, and avenues for collaboration should be identified in order to contribute to the efficiency and effectiveness of the overall nuclear order.

The relevant IAEA treaties, conventions, non-legally binding codes of conduct and United Nations resolutions, as well as the sharing of best practices and resources, are all considered part of today's global nuclear norms.However, what is adopted on paper can be at variance with what is implemented in practice.

An option to consider is the establishment of a review process for such legal instruments or mechanisms in order to achieve a more transparent assessment of States' implementation of their obligations. Before such measures can be achieved, there are other steps to take, such as more active engagement by the IAEA. For example, the IAEA Director General could inform the State in question in writing about the potential risks associated with inadequate implementation of its legal commitments in relation to the legal instruments adopted, which could open a channel for corrective action that could be undertaken.

The proposed changes could be initiated in a number of ways. The IAEA Board of Governors could mandate the secretariat to initiate action. States parties to the nuclear safety and security conventions could also prompt such action during the review meetings on such instruments. The forthcoming International Conference on Physical Protection of Nuclear Material and Nuclear Facilities, scheduled for November, is yet another venue in which we can explore hardening nuclear infrastructure against acts of terrorism.

In addressing risks relating to nuclear security threats, including acts of terrorism, the Nuclear Security Summits have made important contributions. That work continues now, to a great extent, within the IAEA and in cooperation with other international organizations and industries, as guided by the IAEA Ministerial Conference held in Vienna in December 2016, which reaffirmed the importance of protecting nuclear and radioactive material. The Conference adopted a declaration that puts that responsibility in the hands of the international community, international organizations and Member States. In order to fulfil that requirement, the IAEA and other international organizations need adequate funding. To that end, the support of the Security Council is indispensable. The efforts of the Security Council to analyse and assess terrorist threats, highlight existing vulnerabilities, identify capacity gaps with the aim of understanding the challenges posed by terrorism to critical infrastructure, and recommend how best to support Member States in those efforts are essential in combating terrorism.

The President: I thank Mr. Heinonen for his briefing.

I shall now make a statement in my capacity as the Minister for Foreign Affairs of Ukraine.

I would like to thank today's briefers for their inputs into our discussion. Once again, they reconfirmed the complexity and importance of the problem in question.

The protection of critical infrastructure is vital to national security, public safety and the economic development of all States. Terrorist attacks on such facilities and services can significantly disrupt the functioning of societies and bring about massive human suffering.

I would also like to express my appreciation to all Security Council members for their support during the process of preparing the text of resolution 2341 (2017), which was adopted today. The resolution sends a strong message from the Security Council to the international community to give serious consideration to the issue. It also outlines a specific framework of objectives and actions aimed at raising awareness of possible terrorist threats to critical infrastructure. It does so by identifying the threats and preventing them, as well as by seeking to alleviate their possible consequences.

As part of their essential counter-terrorism efforts, it is crucial for States to develop and put in place a strategy that assigns the relevant tasks and responsibilities regarding the protection of critical infrastructure from terrorist attacks. The primary goals should be to counter such attacks and prevent their repetition by identifying the perpetrators and their supporters, as well as to provide support to victims of terrorism.

In view of the existing challenges to international peace and security, especially the evolution of terrorist threats, Ukraine has been working to develop a national legal framework for the protection of critical infrastructure against such threats. Taking into account a series of terrorist attacks in recent years against facilities in Ukraine, that work has become particularly important.

Since 2015, several Ukrainian governmental agencies, as well as critical national infrastructure, such as regional power grids and financial institutions, have become the targets of attacks by malicious software. Hacker groups have also attacked the Kyiv airport and the Ministry of Defence's electronic resources. On 6 December 2016, on the eve of the end of the financial year, the websites of the State Treasury, the Ministry of Finance and the State Pension Fund were temporarily paralysed . Of course, we know that the objective of such attacks is to damage Ukraine's financial system,

weaken our defence capabilities and eventually destabilize Ukrainian society. It is quite obvious that Ukraine has been deliberately selected as a target by organized external cyberterrorists. Their attacks can be as devastating as more conventional warfare. We have been hurt, but we have grown more resilient as a result of the attacks.

In today's dynamic and globalized world, we are of the view that the following elements should be incorporated into national policies in order to maintain an adequate level of safety and resilience for critical infrastructure. The first element is cooperation among all stakeholders, both public and private, involved in the process of operating and protecting critical infrastructure. The second element is the open exchange of information about threats and risks to critical infrastructure among public authorities, the private sector, communities and individual citizens. The third element is to increase the level of self-protection, mutual assistance and self-empowerment of individuals and organizations that can be adversely impacted by the termination or impairment of critical infrastructure services.

Apart from the factors I just listed, a coherent system aimed at averting the terrorist threat to critical infrastructure should prioritize active international cooperation, which would include, inter alia, an exchange of best practices and the holding of joint training sessions and investigations. Such international cooperation has gained paramount importance given the development of global cross-border infrastructure projects. Terrorist attacks against those projects may affect the interests of several States and cause significant damage, both economic and environmental. In that context, our goal must be to intensify cooperation at the national, regional and international levels, and to establish early-warning and rapid-response mechanisms in order to react better to possible terrorist attacks.

However, while seeking to safeguard the most vulnerable parts of our critical infrastructure from terrorist attacks, we should never forget that it is the lives of our citizens that are at stake, which we, as States, are obliged to protect. Therefore, it is our duty to do everything possible to prevent terrorist attacks on critical infrastructure. The well-being of our peoples depends on it. That is the main objective of resolution 2341 (2017), adopted today. Forearmed is forewarned. I count on members' further cooperation on this matter.

I resume my functions as President of the Council.

I shall now give the floor to other members of the Security Council.

Mr. Amendola (Italy): It is a pleasure for me to be here today to engage in this discussion on such a crucial topic. Let me thank the Ukrainian Minister, Mr. Klimkin, for convening today's debate and bringing today's resolution 2341 (2017) to the Security Council for adoption.

The threat posed by terrorism and the need to protect critical infrastructure perfectly serve to describe the complexity of the security challenges that affect us all today. The Security Council called for a comprehensive and pre-emptive approach to address their potential impact on global security. Security involves the resilience of States and the cohesion of public opinion. Indeed, resolution 2341 (2017) allows the international community to fill a critical void. Italy therefore welcomes and supports this initiative.

As previous speakers have underlined based on their experience, terrorists target critical infrastructure in many ways, and at times they succeed in disrupting our way of life. It is a matter of the resilience of the State, of public involvement and the fear that terrorists cause in our societies. Last year, for excample, terrorist attacks at airports in Brussels and Istanbul showed how ruthless and effective terrorist groups can be. The targeting and exploitation of facilities by Da'esh in Iraq is another clear, although qualitatively different, example of very damaging attacks on critical infrastructure. In the framework of Iraq Italy remains committed — and we are proud this — to the protection of the Mosul Dam, which has been targeted by Da'esh since 2014, threatening the lives of hundreds of thousands of people living nearby.

Those are just a few examples, but their impact shows how vital it is for the international community to swiftly act upon this threat. It is a transnational threat that requires a transnational response. Clearly, the United Nations has a prominent role in recognizing — just as we are doing today — the need for international cooperation in coordinating a coherent response, including through regional organizations. First of all, we must identify which targets are critical. Secondly, we must announce cross-border synergies to prevent terrorist attacks and mitigate their impacts. Thirdly, we must respond to the threats with cooperation along borders and among States. Since every chain

is as strong only as its weakest link, international dialogue and partnership involving public opinion and capacity-building are key elements in the protection of critical infrastructure.

As many speakers have already mentioned, at this stage of global affairs the importance of connections means that the infrastructure connecting the people very often has transborder effects on society. Sometimes those connections are stronger than borders, and in respecting and defending borders we must be aware that the fact that the nationalities should cooperate to defend the connections. We are therefore ready to support the role of the United Nations, as the resolution suggests, in identifying and spreading best practices for protecting that infrastructure.

A key element of partnership is information exchange. We know this in Europe, as we are doing with the European Union, and the membership should be made aware of the nature of the threats to a single country when they affect our collective security.

Let me say a few words about the role and relevance of cyberspace, and more generally about information and communication technology. We know that today they have decisive relavance to infrastructure and that they are both a means and a target of terrorism. We believe that we must have a broad understanding about what constitutes an attack on information and communication technology. We are already under attack when we are unable to detect and stop the online planning of attacks and the propaganda of terrorist groups on the Internet. We also recognize that an attack is taking place when a plane or a truck is hijacked, so we must acknowledge that a different kind of attack is taking place when network spaces are hijacked by terrorist organizations. We must be able to balance the free access of our public opinion and civil society, as an extraordinary source for communication and democratic participation with our collective security. It is not easy, but plans for our freedom and security are enhanced with today's resolution.

That brings me to a new alliance that we must emphasize and boost. In this framework, defending critical infrastructure also requires an alliance between the public and private sectors, because the connections driving trade, business and communication also drive our civil society dialogue and, at the same time, our need to protect and defend our security. That is why today's debate and resolution are important. They provide an indispensable international legal framework for such a partnership to be announced and to flourish in our free, open and creative society.

Mr. Abdymomunov (Kazakhstan): Let me express my gratitude to you, Mr. President, for highlighting the need to protect critical infrastructure in the light of the recent change of the tactics, forms and strategies of terrorist organizations witnessed today. The challenge becomes more acute considering the immensely vast scope and categories of critical infrastructure that are vulnerable, from nuclear and energy facilities, commerce, finance and banking to all forms of transportation, to mention just a few. The problem is aggravated because digital and modern information and communication technologies are central to all operations of more than 20 major systems of critical infrastructure having national, regional and global implications.

My delegation would like to present how Kazakhstan is taking precautions on two very important fronts: first, information and communication technologies of public resources, and, secondly, nuclear facilities.

Kazakhstan realizes that modern critical infrastructure is drawing the attention of, and attacks from, international terrorist organizations. Although infrastructure protection is a direct responsibility of our State authorities, we see the need for joint public- and private-sector efforts, together with close cooperation with international and regional organizations, including the United Nations Office on Drugs and Crime, the International Atomic Energy Agency, INTERPOL, the Organization for Security and Cooperation in Europe and NATO, as well as the Shanghai Cooperation Organization and the Collective Security Treaty Organization.

We are also taking care regarding potential energy, business, cross-border and transnational disasters, because of the interlinkages of these areas through information and communication technologies. In such circumstances, we are developing our national system to counter terrorism on the Internet, entitled "Cyber-Shield of Kazakhstan".

Currently, the laws of individual Member States have no common approaches for the understanding of critical infrastructure, and therefore it is necessary to harmonize national legislation so as to adhere to United Nations global norms of critical infrastructure security.

I turn now to another key, critical infrastructure — nuclear infrastructure. Nuclear safety is a key collective responsibility today at the national, regional and global level. Kazakhstan is therefore taking all the necessary measures to ensure the security of such facilities located in its territory and in the region. As a party to almost all international conventions in this field, we call on others to comply with them in good faith.

We are also actively striving to promote an international legal framework to ensure the safe handling of nuclear materials. We are vigilant in protecting critical infrastructure, including infrastructure located on the former Semipalatinsk test site — now the National Nuclear Centre of the Republic of Kazakhstan — and on the BN-350 nuclear facility, with the active assistance of our partners. We are ready to prepare highly qualified specialists, and for that purpose we are establishing a training centre on nuclear safety in Almaty with the support of the International Atomic Energy Agency and the United States Government.

Stringent measures are taken to ensure safety in the construction of the IAEA Low Enriched Uranium Bank on our territory, and in the transportation of nuclear materials. In that connection, I would like to emphasize that Kazakhstan has complied with the requirements of the four nuclear security summits, especially as they relate to the safe use of nuclear energy. We are also adequately securing radioactive sources that terrorists could use to manufacture dirty bombs.

Every effort was made to ensure security at the 28th World University Winter Games, recently held in Almaty, by focusing on the early identification and elimination of threats, and the same is true of the forthcoming Astana EXPO-2017.

I am pleased to report that we are developing close cooperation with the European Programme for Critical Infrastructure Protection, along with the fight against transnational crimes. The country is also active in the Critical Infrastructure Warning Information Network of the European Commission, sharing information on research regarding infrastructure protection.

Kazakhstan stands ready to develop common security schemes acceptable to all States, regardless of their national characteristics and traditions, in order to keep our world and planet safe from the ever-growing threats we face.

Mr. Skoog (Sweden): Let me begin by thanking the Ukrainian presidency of the Security Council for convening today's open debate and for conducting the consultations on resolution 2341 (2017), which we have just adopted. The consensus behind it underlines the open and inclusive process that led to its agreement, as well as the importance that we all attach to that vital issue. Out of respect for all Member States that want to participate in this debate, I will make an abbreviated statement now and make the full version available through other means.

Objects of critical infrastructure have long been attractive targets for terrorist attacks. Through turning off the lights, contaminating or shutting off water supplies, or undermining individuals' willingness to travel, such attacks achieve the core objective of terrorism to cause as much fear and disruption as possible. It is hard to imagine the devastating consequences that a terrorist attack on a nuclear power plant could have on human lives and the environment, both in terms of immediate impact and the long-term effects. Mr. Heinonen has reminded us that that is not a wholly unrealistic scenario.

We live in an increasingly interconnected world. That is particularly true when it comes to our critical infrastructure. Interconnectivity — whether physical or in terms of communications technology — means that the ripple effects of a large attack in one country have the potential to be felt not only in neighbouring countries, but globally. For that reason, today's discussion is all the more timely and relevant. Efforts to protect critical infrastructure from terrorist attacks require cooperation — across borders, across sectors and across public and private stakeholders. Regional and global approaches help build resilience and preparedness. All public agencies in Sweden are required to undertake a security analysis to identify vital critical infrastructure within their remit, and to identify and assess potential risks.

The purpose of our policy is twofold. The first goal is to improve awareness, build resilience and prevent attacks, and to respond and recover from incidents and crises where they do occur. The second aim is to increase cooperation for prevention among all relevant stakeholders, including public and private actors, at the regional and international levels.

Sweden's Counter-Terrorism Cooperation Council brings together relevant actors to jointly increase

national capacity. Our approach involves law enforcement, intelligence and security authorities, the Civil Contingencies Agency, sector-specific agencies, regional and local authorities, and the private-sector actors that own and operate critical infrastructure. In 2016 we launched a national system for the mandatory reporting of information technology incidents for all Government agencies. Next year, as part of the European Union (EU) directive on security in network information systems, such reporting will become mandatory for both public and private actors.

Moreover, at the level of the European Union, the EU and its member States are committed to acting in solidarity within any member State that is the object of a terrorist attack, the so-called solidarity clause. The EU has put in place a range of initiatives to address the protection of critical infrastructure. The approach is not only focused on threats from terrorist attacks, but also on those resulting from criminal activities, natural disasters and accidents. We supports several EU programmes aimed at protecting critical infrastructure within the broader region, which includes the Balkans and Turkey.

There are a number of regional organizations created to improve the capacities of member States in matters related to civil protection and preparedness, such as the Council of the Baltic Sea States, the Arctic Council and the Barents Euro-Arctic Council, which is a forum aimed at supporting and promoting regional cooperation in the northernmost parts of Sweden, Norway, Finland and the north-western parts of Russia. Iceland and Denmark are also members.

There must be accountability for all acts of terrorism. Perpetrators, organizers, and sponsors of terrorist attacks must be held responsible. As reflected in resolution 2341 (2017), adopted today, measures to counter terrorism must be taken in accordance with international law, including human rights law and international humanitarian law.

We welcome the fact that the resolution encourages the Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism, to continue to examine these important issues. The country visits by the Counter-Terrorism Committee Executive Directorate have resulted in valuable knowledge and expertise, and the potential for States to draw on best practices. More, not less, international cooperation is key to countering these threats. We appreciate Ukraine's leadership on these issues in the Security Council.

Mr. Lamek (France) (*spoke in French*): At the outset, allow me to thank Ukraine for having taken the initiative of convening this important debate. I should also like to thank the speakers thus far for their insightful statements.

France associates itself with the statement to be delivered on behalf of the European Union.

The examples of terrorist attacks that have targeted critical infrastructure, particularly transportation, are regrettably numerous, as we were reminded with the tragic attacks on the Brussels airport and Metro in March 2016 and on the Istanbul airports in December 2015 and June 2016.

This debate gives the Council another opportunity to send a strong and united message on the important of international cooperation in the fight against terrorism, as we have already done in other meetings on the financing of terrorism, on the fight against propaganda and on international legal cooperation. The fight against terrorist threats must be waged on all fronts, with respect for international law and for States' national authorities. It is especially necessary for each State to have robust preventive and protective measures in place in order to deter terrorists from carrying out attacks against potentially vulnerable targets or, failing that, in order to be able to react rapidly and effectively when they do occur.

France considers protecting the people and ensuring the continuity of the essential national functions to be a strategic priority. In 2006, we set up a security mechanism for vital activities in order to protect them from malicious acts, such as terrorism. Today there are more than 200 public and private entities classified as organs of vital importance that are subject to special rules and vigilance. The list of ths infrastructure is kept confidential and includes administrations, media, transportation entities and industrial actors in different sectors. They ensure activities that are crucial to the functioning and the survival of the nation.

In that context, France welcomes the unanimous adoption of resolution 2341 (2017), the first to be so closely concerned with this key topic. I draw the Council's attention to two messages contained therein.

The first involves the prevention of and preparation for potential threats. Early identification of the major

challenges and vulnerabilities in terms of protecting critical infrastructure, and the elaboration of a targeted strategy to be implemented in the event of an attack are essential. Such approaches help not only to reduce risks, but also to improve responsiveness.

The second message concerns the observation that strengthening critical infrastructure protection cannot be done in isolation. Cooperation, whether intra- or inter-agency or among States, is essential in order to ensure an adequate level of protection. That includes exchanging information, knowledge and experience. Owing to the very nature of the activities carried out by critical infrastructure, close cooperation between the public and private sectors is absolutely essential.

There are many challenges. But the scale and particularly high level of the terrorist threat today must prompt us to strengthen our efforts to protect populations and to ensure the continuity of crucial State services.

Allow me to conclude by thanking once again the Ukrainian presidency of the Security Council for this very useful debate on a question that is both specialized and technical, but also touches on the daily lives of all our fellow citizens. Rest assured that France will continue to play its full part in such efforts.

Mr. Seck (Senegal) (*spoke in French*): At the outset, I should like to convey the sincere gratitude of the Senegalese delegation to the Ukrainian presidency for having taken the initiative to organize this important debate on a topic of proven relevance. The briefings of this morning made by Ms. Viotti, Mr. Stock, Mr. Rao and Mr. Trelawny have given us a clear idea of the issues under consideration, and I would like, on behalf of the delegation of Senegal, to warmly thank and congratulate them.

I recall that in September 2016 we held an open debate concerning aviation security in the face of terrorist attacks (see S/PV.7775). We also held two Arria Formula meetings in November, one of which was organized by Ukraine on the topic of critical infrastructure. The other, on the issue of cybersecurity, was co-organized by Senegal and Spain. Our discussion this morning affords us an opportunity to continue our strategic analysis of the ways and means to properly identify and better prevent the risks linked to such threats and, at the same time, to measure the reliability, resilience and vulnerability of critical infrastructure in the face of terrorist attacks that could lead to incalculable catastrophe.

Because extremist groups have increasingly targeted civilian infrastructure in their efforts to maximize civilian casualties, such infrastructure should be given priority in terms of surveillance and protection in order to preserve the continued operation of human communities and enterprises, while also guaranteeing national security and public safety in countries that are targeted or attacked. On that point my delegation welcomes the unanimous adoption this morning of resolution 2341 (2017), which constitutes, without a doubt, an important step forward in the international community's efforts in the face of such emerging threats to international peace and security.

Given the interconnected nature of civilian infrastructure, which only serves to heighten its vulnerability, constant vigilance and awareness — bearing in mind the specificities of the geopolitical environment and context of each country and region — is crucial. The delegation of Senegal thinks that it is very important to establish and strengthen public-private partnerships at the national, regional and international levels with all stakeholders, in terms of sharing information, experience and even intelligence, as well as operational coordination, the securing of supply lines and border control. I would like to recall that Senegal has established a framework for the exchange of sensitive information with other States with a view to coping more effectively with the emergence of new threats and attempts at illicit actions using aircraft or targeting airports or port infrastructure.

In the area of aviation, in accordance with the provisions the relevant texts adopted by the International Civil Aviation Organization, which stipulate that each State is responsible for the effective implementation of all safety measures aimed at protecting civil aviation against illegal attacks, Senegal has for several years implemented a broad programme aimed at enhancing civil-aviation security in the country and in its airspace. That policy has led the national assembly to adopt a new civil aviation code through an act of 4 May 2015 and to establish aircraft regulations aimed at ensuring the full implementation of security procedures and measures.

In the maritime and ports sphere, I wish to point out that Senegal is a signatory to most of the international instruments mentioned by the Special Adviser to the Secretary-General, including the Yaounde process, the

Djibouti Code of Conduct and the African Charter on Maritime Security, Safety and Development, adopted in October 2016 in Lomé.

At the subregional level, a cooperation agreement was signed on 24 March 2016 by the relevant Ministers of Senegal, Mali, Côte d'Ivoire and Burkina Faso in order to pool the efforts of those countries; strengthen cooperative relations among their security services and establish unity of action through the harmonization of national counter-terrorism legislation and border surveillance; and ensure the authenticity of travel documents in accordance with regional agreements concerning the movement of persons.

Over the past few years, West Africa has seen an increase in terrorist attacks and criminal cyberattacks. In that regard, I would mention the report of the United Nations assessment mission on the impact of the Libyan crisis on the Sahel region, carried out in December 2011 (see S/2012/42), in which the circulation of a large number of weapons and ammunition in the region was noted, in particular rocket launchers. Such smuggled weapons constitute a real threat to the security and stability of the Sahelo-Saharan region. It is therefore essential to avoid having Africa become the weak link in preventive efforts to protect and secure critical infrastructure. On that point, the delegation of Senegal welcomes and strongly supports the effective implementation of paragraph 9 of the resolution that we have just adopted.

Moreover, the Counter-Terrorism Committee, which is already doing outstanding work through its Executive Directorate in cooperation with the Counter-Terrorism Implementation Task Force, should continue to provide technical assistance to affected States in order to help them strengthen their capacity to protect critical infrastructure and vulnerable public spaces.

In conclusion, my delegation would like to point out that, for the implementation of the resolution we have just adopted to be effective, it must be consistent with previously adopted Council resolutions in the framework of the fight against terrorism, in particular resolutions 2178 (2014), 2253 (2015) and 2322 (2016). Hence, it should be part of a more comprehensive United Nations global anti-terrorism strategy. My delegation is also waiting with great interest for the presentation in the coming 12 months by the Counter-Terrorism Committee of a progress report on the implementation of the important resolution just adopted.

Mr. Bessho (Japan): I would first like to express my sincere appreciation to you for taking up this timely and important topic. My appreciation also goes to Ms. Viotti and all other speakers for their insightful briefings.

Over the past few months, we have adopted two Security Council resolutions on counter-terrorism: 2309 (2016) on aviation security and 2322 (2016) on international judicial cooperation. We welcome the adoption today of resolution 2341 (2017), on the protection of critical infrastructure. We thank Ukraine for taking the lead. Through these resolutions, the Security Council has shown unity in addressing terrorism through a multifaceted approach. Our task now is to translate these resolutions into action.

Once a terrorist attack occurs, it is already too late, especially given the devastating impact that the destruction of critical infrastructure could have on societies and individuals. We must collectively strengthen our security with a focus on prevention. Japan is giving particular priority to the protection of critical infrastructure. We owe it to our citizens and visitors alike. This is especially so for Japan, as the host of the Tokyo Olympic and Paralympic Games in 2020 and the Rugby World Cup in 2019.

Learning from international best practices, Japan has enhanced its infrastructure security, including for public transportation, large-event facilities, international seaports, nuclear plants and embassies. The protection of nuclear plants from terrorist attacks is particularly important owing to the possibility of a particularly devastating effect. For nuclear plants in Japan, anti-firearm squads are deployed by the police around the clock and special assault teams can be dispatched in emergencies. Information is key. Japan is exchanging information with foreign counterparts and police are conducting joint exercises with self-defence forces while also working closely with nuclear plant operators through on-site visits and guidance on self-vigilance.

Responding to recent technological developments is critical. As there has been an increase in incidents involving the malicious use of information and communications technologies, Japan has been enhancing its cybersecurity in cooperation with the private sector and foreign counterparts. Last April, we enacted a law prohibiting unmanned aerial vehicles, or drones, from flying over critical facilities, embassies and nuclear plants to prevent possible attacks.

Our experiences attest to the importance of multiple streams of efforts, including international and public-private cooperation, accelerating information exchange, sharing good practices, developing advanced technologies and supporting capacity-building for those in need. We believe the resolution just adopted provides a useful framework for all other members to undertake their own proactive efforts. As part of this effort, two weeks ago the Government of Japan decided on a new assistance package for international cooperation in the fields of counter-terrorism and preventing violent extremism. This will be used to facilitate the implementation of relevant Security Council resolutions through concrete projects, such as a project on cyberattacks on information technology systems of financial infrastructure. We also support the initiative of Secretary-General Guterres to ensure coordination and coherence in United Nations counter-terrorism efforts, under the United Nations Global Counter-Terrorism Strategy review process.

To conclude, I would like to emphasize Japan's consistent and constant preparedness to promptly address terrorism in all its aspects. Japan will continue to be an active partner in this important endeavour with the entire international community.

Mr. Alemu (Ethiopia): We would like to express appreciation to the Ukrainian presidency for organizing and to you, Mr. President, for presiding over this important debate on the protection of critical infrastructure from terrorist attacks. We welcome the unanimous adoption of resolution 2341 (2017) and our thanks also go to all the briefers for their presentations.

With the growing threats of terrorism and violent extremism, the vulnerability of critical infrastructure to attacks by terrorists has been a source of great concern. The devastating economic and security impact of such attacks to some of the infrastructure that we normally take for granted in our daily lives, such as water, electricity, telecommunication and the Internet, transportation, banking and finance is too ghastly to contemplate. Of course, the airline industry has often been the primary target of terrorists and a series of measures have already been put in place to enhance aviation security. However, the airline industry still remains vulnerable to terrorist attacks; hence the need for greater international cooperation in closing any loopholes that could be exploited by terrorists.

We all know that terrorists and other criminals have developed the capacity to launch coordinated and sophisticated attacks on other critical infrastructures. Public institutions, private businesses, factories and industries, roads and bridges, shopping malls and sport centres, among others, have increasingly become targets of attacks aimed at disrupting normal economic activities. Cyberterrorism carried out with the aim of causing damage to computer systems and telecommunication infrastructure has also become a real danger.

All countries big and small are indeed vulnerable to these kinds of threats. As we are living in a volatile neighbourhood, which is facing threats of terrorism and violent extremism, attacks against critical infrastructure by terrorists are not remote possibilities for us. They are real threats and they have already happened in our region. We believe it is through effective international cooperation that the protection, security and resilience of critical infrastructure can be enhanced.

The protection of critical infrastructure can be said to have been partly addressed by international treaties and conventions related to civil aviation, maritime security and nuclear weapons. However, there has not been a resolution dedicated to this issue, and the resolution we adopted today will, we hope, fully contribute to promoting greater international cooperation to effectively counter terrorist attacks against critical infrastructure.

As the concept note (S/2017/104, annex) rightly points out, there is a need to build national capacity to prevent and react to potential risks and threats in this regard. The roles of the Counter-Terrorism Committee, along with its Executive Directorate and the United Nations Counter-Terrorism Implementation Task Force (CTITF), will be critical in closely following up on this issue and helping Member States build their capacities. The designing of tailor-made programmes on the protection of critical infrastructure by CTITF, in line with the potential threats and risks they face, could certainly be very helpful. Reactivating the CTITF Working Group on the Protection of Critical Infrastructure Including Internet, Vulnerable Targets and Tourism Security will be instrumental in achieving this objective; no doubt, so would be the very timely initiative that the Secretary-General is contemplating to enhance the capacity of the Secretariat to better coordinate the United Nations counter-terrorism effort, which indeed has so far lacked coherence.

Finally, we believe that the sharing of experiences and best practices among countries and regions could also go a long way in enhancing capacity and responsiveness to such threats. The United Nations in cooperation with regional and subregional organizations could possibly facilitate such platforms to enhance their awareness and enable the exchange of valuable experiences in connection with the protection of critical infrastructure.

Mr. Bermúdez (Uruguay) (*spoke in Spanish*): I thank you, Mr. Minister, for presiding over our work today. I would like to commend your country for having organized this open debate and for conducted with great balance and transparency the negotiations on the important resolution 2341 (2017), which we adopted today and which, together with resolution 2309 (2016) on the terrorist threat to civil aviation, reflects the importance that the Security Council attaches to the issue. I would also like to thank the Chef de Cabinet of the Secretary-General, Ambassador Maria Luiza Ribeiro Viotti, for her participation and all the other briefers at today's debate for their informative briefings.

There is growing concern on the part of the international community with regard to the threat of terrorist attacks against critical infrastructure. That concern is highly justified when we consider the serious consequences that such acts may entail in terms of the loss of life and the elimination of or the decreased ability of States to provide essential services to their population and economic losses. The actions carried out by those terrorist groups through the use of new technologies and increased capabilities extend beyond borders and regions, which forces us to adopt measures to confront those new challenges. It is therefore no surprise that at the State, regional and international levels, initiatives aimed at protecting infrastructure, taking into account both physical and cybernetic aspects, are gaining ground.

It is also necessary to generate greater public awareness concerning cyberthreats and their potential consequences through involving all public and private stakeholders and promoting cooperation and coordination among them. Furthermore, we undeniably find ourselves in an are that requires greater legislative development both at the domestic and international levels. As we have already seen in other areas in the fight against terrorism, inter-State, regional and international cooperation is essential for the success of preventive policies on attacks of that nature as well as for the containment of their potential consequences. That is becoming increasingly necessary as many States face difficulties and constraints with regard to applying and implementing effective policies owing to insufficient material resources and the lack of trained personnel and practical experience in assessing threats, risks, vulnerabilities and consequences. Accordingly, a greater exchange of information and experiences, knowledge of best practices, technical assistance and, in some cases, financial support are also necessary.

It is important to create areas of discussion and seek effective prevention measures, thereby supporting the work already being done by the United Nations through its competent bodies. We also believe it is relevant to underscore that critical infrastructure must be protected wherever it may be. Uruguay was a sponsor resolution 2286 (2016), on the protection of hospitals and humanitarian personnel in situations of armed conflict, and attaches particular importance to that issue.

In Latin America, several countries already have a strategy and legal framework for cybersecurity and cyberdefence, and others have begun to develop national and comprehensive policies and strategies concerning cybersecurity. In 2004, the members of the Organization of American States (OAS) unanimously adopted the Comprehensive Inter-American Cybersecurity Strategy, and in 2012 they signed the Declaration Strengthening Cybersecurity in the Americas. Similarly, in 2015 the Inter-American Committee against Terrorism of the OAS adopted the declaration on the Protection of Critical Infrastructure from Emerging Threats.

Uruguay has its own response centre to respond to cybersecurity threats that coordinates and implements the response to that type of incident and develops and disseminates policy standards and best practices in order to increase security levels. In tandem with the Government's electronic agency for the country, it collaborates with other countries and has joined international bodies with a view to bolster communication and cooperation among response centres. That is the case of the Inter-American Committee against Terrorism and the specialized United Nations Regional Inter-agency Working Group on Information and Communications Technologies. At the level of the Ministry of the Interior, there is a department of technological crimes, and in April 2015 we established a response defence centre for cybersecurity incidents in the Ministry of Defence. In

the first quarter of 2016 in Uruguay, there was total of 419 incidents of cybersecurity incidents, which accounted for an 11 per cent increase compared to the same period for the previous year. Among other factors, that increase is attributed to the global trends relating to cyberattacks and cyberfraud.

It is undeniable that the capacity of Member States to respond to terrorist attacks against critical infrastructure remains uneven owing in large part to its varying degrees of development and the availability of resources. We must therefore must be aware of the collective duty to provide protection as well as the respect for the sovereignty of States while ensuring the right balance between security measures and the protection of human rights and fundamental freedoms.

Mr. Klein (United States of America): I want to thank all the briefers for their very informative and comprehensive briefings today and for highlighting the work that their organizations are doing on this important topic.

The United States recognizes Ukraine for drawing attention to the importance of protecting critical infrastructure. The challenges for most people is that critical infrastructure is both everywhere and nowhere. We do not think about the bridges and the tunnels that allow us to get to work every day. We do not think about the radars, satellites and radios that allow aeroplanes to move safely across the sky. We do not think about the network of power plants, substations and high-voltage lines that keep the lights on. We do not think about the server rooms and fibre-optic cables that get our e-mails to where they need to be. Therefore, when we talk about protecting critical infrastructure at the Security Council, we are really talking about nothing less than protecting what underpins our daily lives in the modern era.

It is not an issue that each of us can combat in isolation, and that is why the United States supported resolution 2341 (2017), adopted by the Council just moments ago. Part of the reason, of course, is that the consequences of an attack on critical infrastructure could go far beyond one country's borders. Pipelines carrying vital supplies of oil and gas span thousands of miles. A catastrophe at a chemical or nuclear plant could sicken people across continents. One could go on and on, but the point is that protecting critical infrastructure can help keep us all safe. Another reason, however, to cooperate is that the threat to critical infrastructure can be transnational. That is especially true of cyberthreats whereby malicious actors can reach across borders to cause havoc. We can therefore surely agree on the importance of this issue and its international dimensions. The question then becomes how Member States can act to reduce the risk of a devastating terrorist attack.

In the United States, private companies own most of the country's critical infrastructure, and that is why protecting it is a shared responsibility among various levels of Government, companies and individual citizens. It has to be a collaborative effort. In fact, anyone in the Chamber who has ridden a New York City subway has certainly seen all the signs reminding passengers: "If you see something, say something". That is part of the strategy. Every bit of extra vigilance can help. The United States Government, especially the Department of Homeland Security, is constantly working on public-private partnerships that strengthen the resilience of our communities. The United States believes that the United Nations counter-terrorism bodies and its agencies can be helpful. They can collect information on how Member States can address critical infrastructure and disseminate best practices for keeping these institutions safe.

Today's resolution also recalls that the States Members of the United Nations must ensure that terrorist attacks are criminal offences, including those intended to destroy or disable critical infrastructure. That is important partly for deterrence, but also to make sure that perpetrators of such attacks cannot escape prosecution. Member States must strengthen partnerships to share information about potential threats and ensure that their law enforcement and other relevant agencies can work together to prevent attacks before they happen. As the Minister said, forewarned is forearmed.

This is a new area of cooperation for the Security Council to discuss, and so there is still much that we still need to define, including the role of the United Nations in helping Member States cooperate. But the resolution today should be an impetus to develop concrete ways for Governments to share the lessons they have learned and to collaborate in keeping critical infrastructure running safely in the background of our daily lives, where it should be.

Mr. Aboulatta (Egypt) (*spoke in Arabic*): At the outset, I should like to express my sincere thanks and

congratulations on the adoption of the significant resolution 2341 (2017), on the protection of critical infrastructure from terrorist attacks. I would also like to thank the Ukrainian presidency of the Security Council for convening this important debate. And I also thank the briefers for their valuable presentations.

The terrorist incidents witnessed by the world today attest to the importance of protecting critical infrastructure, which ought to be a priority as part of our efforts to counter terrorism, especially with the increasing numbers of victims of terrorist incidents that target infrastructure. Such attacks also have a negative impact on large segments of the peoples subjected to such attacks — one that goes beyond national boundaries.

Today's resolution is the first of its kind to address the protection of critical infrastructure against terrorist attacks. It covers a number of important points that must be taken into consideration, including the fact that every State must determine what constitutes its critical infrastructure, especially given the absence of an international definition in this area, as well as how to effectively provide protection from terrorist attacks. The resolution also reiterates the need for inter-State cooperation, promoting international cooperation and information exchange and increasing awareness so as to improve preparedness to counter attacks against critical infrastructure.

The resolution also underscores the importance of every country identifying and developing strategies to eliminate terrorist risks to critical infrastructure. The resolution urges States with capacity to provide relevant assistance to build the capacity of other States and empower them to protect their critical infrastructure against terrorist attacks, including through training and providing the necessary resources, as well as technical assistance and the transfer of technology.

The adoption of this resolution on protecting critical infrastructure against terrorist attacks is of vital importance. However, more crucial is implementing this and other Security Council resolutions on counter-terrorism. That requires thorough follow-up by the Council and the holding to account of countries and regimes in the event of non-compliance when it comes to implementing such resolutions, or in the case of those who finance or sponsor terrorism or who harbour or supply them with weapons. Such countries and regimes are sapping our efforts and riding roughshod over the resolutions adopted by the Council to defeat terrorism. It is high time to hold them accountable for sponsoring terrorism.

In conclusion, allow me once again to thank the Ukrainian presidency and to assure the Council that Egypt will remain committed to its obligations and will be at the forefront of the efforts of the international community to defeat terrorism, while respecting international law, the rule of law and human rights.

Mr. Rycroft (United Kingdom): I am most grateful for the analysis shared by the briefers this morning. I join others in paying tribute to you, Mr. Minister, for your leadership in bringing this important issue to our attention.

The terrorist threat has evolved over the past decade. We face increasingly complex threats as terrorists acquire new knowledge and new technology. Not content with simply killing innocents, terrorists seek to destabilize, demoralize and disrupt our way of life. Critical infrastructure, be it a transport system, a communications hub or a power grid, represents an attractive target for these sinister actors. The fact that those responsible for the attack on the Brussels metro and airport last March had also invested time and surveillance on a Belgian nuclear scientist should concern us all. We must redouble or vigilance to ensure that we are ready to defend the systems that allow our societies to function.

We therefore wholeheartedly welcome the action taken by the Security Council today to adopt resolution 2341 (2017). The resolution raises the profile of this important issue, calls on States to improve preparedness and strengthens our cooperation in protecting the security of our people and our critical infrastructure. If we are to truly tackle this threat, I believe we need to focus on three things, namely, preparation, protection and partnerships.

First, on preparation, it is vital that plans for protecting our critical infrastructure be comprehensively developed, maintained and tested. We echo the call of the resolution for States to develop their own strategies to prepare and respond to any attack. Threats to our infrastructure can come from many sources: terrorism, criminality or natural hazards. In reducing the risk to our infrastructure, the United Kingdom takes an all-risks approach. That means developing plans that can be used to respond to many types of disruption or threats to life. Measures taken by States to prevent unlawful or

criminal interference in our infrastructure can also serve to help prevent terrorist attacks. It is in part because of the strong measures we have taken that terrorist threats to our infrastructure are being mitigated.

Secondly, on protection, the threat to some elements of our national infrastructure may be aspirational, but there is one area where the threat is very real and very high, that is, transport. As recent reports by the Secretary-General show, there continues to be a serious and enduring threat from international terrorism to our transport networks, specifically to civil aviation. Three billion passengers reach their destinations by air every year. The past year offered us too many reminders of the risks they face: attacks on airports in Brussels and Istanbul, the destruction of the Russian Metrojet aircraft over Sinai and the explosion on board a Daallo Airlines flight from Mogadishu. It was to combat such threats that the United Kingdom authored resolution 2309 (2016), and why today we echo our call on States to work with the International Civil Aviation Organization. Working together we can ensure not only that international security standards keep pace with the terrorist threat, but also — crucially — that they are implemented effectively on the ground.

Finally, on partnerships, the critical infrastructure that we need to protect is largely owned by the private sector, and can also form part of complex international networks and supply chains. Preparation and protection of infrastructure are simply good intentions if we fail to work across sectors to achieve them. Each side has its part to play. Private companies are responsible for ensuring that their infrastructure is protected and that essential services are maintained, just as Governments have an obligation to ensure that industry is managing these risks fully and responsibly. As today's resolution identifies, stronger international partnerships are vital at a time when the functioning of infrastructure relies on cross-border networks and supply chains. The sharing of information, early-warning networks and expertise will strengthen our common approach.

The Security Council needs to stay abreast of the evolution of the terrorist threat and respond to it. Just as we act to prevent conflict, we should also act pre-emptively to prevent terrorism. Today we have put another building block in place to strengthen our common effort. Because of our efforts, terrorists intent on stirring chaos have another hurdle to cross. Because of our efforts, our societies are little safer than they were yesterday.

Mr. Liu Jieyi (China) (*spoke in Chinese*): China appreciates Ukraine's initiative to convene today's open debate of the Security Council on the protection of critical infrastructure against terrorist attacks. We welcome Foreign Minister Klimkin's presiding over the meeting. We listened attentively to the briefings made by the Secretary-General's Chef de Cabinet, Ms. Viotti, and the other briefers.

With the deepening of economic globalization and the interconnection of countries becoming increasingly close, infrastructure is of great significance for countries as they develop their economies and strengthen interconnectivity and economic integration. On the other hand, the global counter-terrorism situation is increasingly serious, and infrastructure is increasingly becoming an easy target for terror attacks. Recently, a series of terrorist attacks on infrastructure, such as airports and mass-transport stations, has caused panic and resulted in serious losses of life and property. The international community should pay close attention to such developments and work together to fight this phenomenon.

First, countries need to focus on ensuring the security of regional interconnection projects and other critical infrastructure. Regional collaboration has significant bearing on global economic development and prosperity. China's Belt and Road Initiative makes infrastructure interconnection a cooperation priority with a view to supporting the countries along the Road, improving their infrastructure development and achieving mutually beneficial win-win cooperation and synchronized development for the benefit of everyone. To date, more than 100 countries and international organizations have joined the Belt and Road Initiative. China hopes to strengthen cooperation in areas such as intelligence-sharing, risk assessment and joint law enforcement through bilateral and multilateral channels, in accordance with the relevant resolutions adopted by the Security Council and the General Assembly, so as to effectively protect interconnection projects and transboundary infrastructure from terrorist attacks and to ensure the safety and security of the Belt and Road construction.

Secondly, countries need to effectively assume primary responsibility for the protection of their infrastructure. China hopes that, in accordance with the requirements of resolution 2341 (2017), countries will strengthen their coordination and develop relevant national-security policies, factoring in the risk of terror

attacks so as to strengthen their capacity to protect infrastructure from such attacks through monitoring, early-warning systems and emergency response, with a view to ensuring the safety and security of their infrastructure.

Thirdly, countries need to strengthen international cooperation in the area of infrastructure security. Countries need to comprehensively strengthen relevant international cooperation from the vantage point of building a human community of shared destiny. Developed countries should help developing countries strengthen capacity-building in that regard. Parties need to strengthen cooperation in information-sharing, law enforcement and judicial assistance in order to crack down on terror attacks against infrastructure. Relevant international and regional organizations should help Member States to share best practices and enhance national prevention capabilities. The United Nations and the Security Council should play a leading role in the relevant international cooperation.

Terrorism is the common enemy of all humankind. Whenever, wherever and in whatever forms it occurs, it must be countered resolutely. Countries need to adhere to uniform standards and staunchly crack down on all terrorist organizations listed by the Security Council. International counter-terror actions should maximize the leading role of the United Nations and its Security Council and abide by the purposes and principles of the Charter of the United Nations so as to enhance effective coordination. China, as an important member of the international counter-terrorism camp, will continue to pursue bilateral and multilateral cooperation in accordance with its national law on counter-terrorism and the relevant international conventions in order to ensure the effective protection and security of infrastructure and work with the international community to combat terrorism and safeguard international peace and security and stability.

Mr. Zagaynov (Russian Federation) (*spoke in Russian*): I too should like to thank the briefers for their participation in today's meeting.

Combating terrorism in today's world must be an absolute priority in the work of the Security Council. Today, the international community is encountering increasingly sophisticated forms of terrorist activity and support. The Islamic State in Iraq and the Levant (ISIL), Jabhat al-Nusra, Al-Qaida and their allies are adapting themselves to the changing situation, introducing new forms of financing and expertly using modern information technologies to develop their material base and attract recruits. The Security Council should do everything it can to counter those new threats.

Guided by those principles, our delegation has put forward a whole range of initiatives in the Security Council. In implementing many of those initiatives, we have relied upon the counter-terrorism structures of the United Nations and Member States, including, in particular, a number of measures to combat the financial resourcing of terrorism, which are set forth in resolution 2199 (2015). Further, important steps for combating ISIS and its financing were envisioned in resolution 2253 (2015), which was put forward by Russia and the United States.

A number of terrorist threats today remain without an appropriate response. The coordination of the efforts of the members of the international community in that area would contribute to setting up the broad international anti-terrorism coalition that has been proposed by the Russian Federation. We have introduced a draft resolution in the Security Council on combating terrorist ideology with a focus on the spreading of that ideology through the Internet. Those approaches have the support of many members of the Security Council. Our delegation has also always supported proposals aimed at finding the most effective measures to combat the modern challenge of terrorism.

At the same time, we believe that in preparing new decisions of the Security Council, especially in as important an area as combating terrorism, the focus should be on truly important topics, with attention to added value and the achievement of concrete results. It is not worthwhile to start negotiations that seek merely to outline obvious points or reproduce statements that have already been submitted many times in other international or national documents. Of course, there is no harm in that approach, but no real results have ever come from such efforts.

We call once again on members of the Council to work resolutely and in a coordinated manner in order to develop effective and joint responses to the pernicious challenges of terrorism that come, first and foremost, from ISIL, Jabhat al-Nusra and Al-Qaida, and the groups connected with them. The acuteness of those threats has not diminished.

Mr. Arancibia Fernández (Plurinational State of Bolivia) (*spoke in Spanish*): At the outset, I would like to welcome Foreign Minister Klimkin today and thank the delegation of Ukraine for having put this item on the Security Council's agenda. I would like to express my thanks and appreciation to all of the speakers who have taken the floor before me.

The Plurinational State of Bolivia reiterates its firm commitment to the fight against terrorism and its categorical rejection of terrorist acts, regardless of why, where or by whom committed, if they are deliberately carried out against international peace and security and in flagrant violations international law. At the same time, Bolivia reiterates that this scourge should not be linked to any religion, nationality, civilization or ethnic group.

The objective of this debate is to encourage Member States to assess their vulnerabilities and interdependence, the impact of terrorist attacks on critical infrastructure and their ripple effects. We are also invited to consider possible preventive measures in the development of national policies and strategies. My delegation participated in negotiations on resolution 2341 (2017), on the protection of critical infrastructure against terrorist attacks, which was adopted today, and wishes to highlight several aspects of the resolution.

We recall the Security Council's resolutions in response to the serious global threat of terrorism, beginning with resolution 1373 (2001), reaffirming the Council's respect for the sovereignty, territorial integrity and political independence of all States pursuant to the Charter of the United Nations. We stress the importance of implementing the United Nations Global Counter-Terrorism Strategy, established by General Assembly resolution 60/288 of 8 September 2006, wherein we reiterated the need to adopt measures to prevent and combat terrorism, and in particular pillar II of the Strategy, which includes the need to strengthen efforts to improve the security and protection of vulnerable targets such as public infrastructure and spaces.

We also recognize that every State identifies that which constitutes its own critical infrastructure and how to protect it effectively against terrorist attacks. We further believe that it is principally the responsibility of Member States to respond to terrorist attacks on what they consider to be their critical infrastructure, be it private or public, and always under national legislation. We support the efforts of the Counter-Terrorism Committee (CTC), with the support of its Executive Directorate, in pursuit of their relevant work in the implementation of resolution 1373 (2001), including support for Member States and the protection of critical infrastructure against terrorist attacks with a view to identifying good practices, gaps and vulnerabilities in that area. In that regard, we encourage the CTC to continue to work, with the support of the Counter-Terrorism Implementation Task Force, to facilitate the provision of technical assistance and capacity-building and to raise awareness of the need to protect critical infrastructure against terrorist attacks, in particular by strengthening dialogue with competent regional and subregional organizations that work closely with one another, especially through the exchange of information.

The legal architecture relating to terrorism has grown with the proliferation of terrorist incidents throughout the world. It is important to acknowledge the efforts of Government and peoples to counter this scourge.

Lastly, we believe that it is important for States to assume their responsibilities in the fight against terrorism, including the protection of critical infrastructure, through full compliance with the provisions of international instruments and the relevant resolutions of this multilateral forum, as well as the effective implementation of the United Nations Global Counter-Terrorism Strategy.

The President: I wish to remind all speakers to limit their statements to no more than five minutes in order to enable the Council to carry out its work expeditiously. Delegations with lengthy statements are kindly requested to circulate the texts in writing and to deliver a condensed version when speaking in the Chamber.

I now give the floor to the Minister for Foreign Affairs of Estonia.

Mr. Mikser (Estonia): I would like to start by thanking Ukraine for organizing this very timely discussion today.

Estonia aligns itself with the statement to be delivered by the observer of the European Union. We are also a sponsor of resolution 2341 (2017), on the protection of critical infrastructure from terrorist attacks.

Our common goal is to make sure that security is not a luxury item; it must rather be a commodity

available to everyone. Even though the terrorist threat in Estonia has remained low, we have been and will be deeply affected by acts of terrorism both in our region and further afield. Estonia therefore remains committed to our common efforts in the fight against terrorism.

Terrorism is an alarmingly increasing phenomenon, both in scope and in geography. Over the past year, we have seen a series of horrific acts of terror all over the world, including in our region, Europe. Several of these attacks have been committed against critical infrastructure. We all remember the heinous attacks on the Brussels and Istanbul airports, where many innocent lives were lost. Indeed, objects of critical infrastructure — such as banks, telecommunications, water and energy supply, transport and emergency services — are attractive targets for terrorists. The vulnerability of critical infrastructure is exacerbated by its increasing dependence on information and communication technologies in an increasingly interlinked world. Attacks against those objects, including cyberattacks, could therefore result in serious damage and loss of life.

Estonia knows what it means to be the target of a large-scale cyberattack. In 2007, our preparedness and swift action prevented major damage to our infrastructure. However, the cyberattacks against Estonia that year clearly highlighted the importance of tackling cybersecurity as part of our national security architecture.

One key word in addressing this threat is resilience. In terms of critical infrastructure, resilience requires the close involvement of the private sector, which often owns and operates these vital services. In some areas, such as banking, cybersecurity has become an integral part of operations, but a similar degree of attention to cybersecurity should be given to other sectors. It should also be understood that, as Governments, we cannot expect information-sharing to be a one-way street from companies to Governments. To build trust, enhance security and share best practices as well as information about possible threat vectors, Governments must also share information with the private sector.

In addition to public-private cooperation, civil society plays an extremely important role in building resilience. In order to effectively strengthen our societies, Governments have to communicate potential threats to critical infrastructure to their citizens and to ensure their readiness to cope with the consequences of possible attacks. One major contributor to our successful handling of the 2007 cyberattacks was horizontal cooperation between information security experts. This led to the establishment of the Cyber Defense Unit of the Estonian Defence League — an innovative model for the involvement of volunteers in national cyberdefence.

It is crucial for countries to map out their critical infrastructure and cross-border dependencies in order to strengthen their national cybersecurity and resilience. No country can face the full spectrum of cyberthreats alone, and international cooperation is crucial to preventing worst-case scenarios. We therefore encourage countries further to share knowledge and contribute to capacity-building across borders, supporting wider acknowledgement of cybersecurity threats and their mitigation.

Estonia has extensive experience in leading and contributing to various cybersecurity and digital development capacity-building efforts globally. We will continue to share our best practices and lessons learned. Here at the United Nations, we are proud to contribute to cybersecurity through the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Cooperation that is all-inclusive is the foundation of resilience. This ensures that the critical players in cybersecurity — Governments, militaries, intelligence, critical infrastructure operators and key private-sector players — are fully informed, prepared and sufficiently capable of handling large-scale cyberattacks.

I would like to reiterate the importance of the Budapest Convention on Cybercrime. The Budapest Convention is the only binding international instrument dealing with cybercrime, and it also covers the use of the Internet for terrorist purposes. The effective implementation of the Cybercrime Convention would ensure that national legislations provide appropriate sanctions for cases involving serious attacks, including terrorist ones, on information-technology-based or general information-technology infrastructure.

Estonia calls on every country to adopt policies, strategies and regulations that help to achieve and maintain an open, resilient, secure and peaceful cyberspace. We must meet the highest standards of due diligence in the development and use of information and communications technology.

Prevention is the only means of preventing radicalization and recruitment into terrorist organizations altogether, as well as of eliminating the terrorist threat to critical infrastructure. We support the Secretary-General's Plan of Action to Prevent Violent Extremism. The prevention of future threats should be given the highest priority in every country.

In line with this, I would like to commend the Secretary-General's initiative to consolidate and streamline United Nations counter-terrorism structures while improving their transparency. We hope that the new structure will also focus on the prevention of violent extremism as its main objective.

The President: I now give the floor to the representative of Slovakia.

Mr. Ružička (Slovakia): I wish to thank you, Mr. President, for holding this debate on the protection of critical infrastructure against terrorist attacks and on promoting discussion on preventive measures against such attacks. In this context, I would like to recall the outcome of the Arria Formula meeting on cybersecurity and international peace and security organized by Spain and Senegal in November 2016.

As the threat landscape changes and becomes more complex, so too must our approach to security problems change in the face of asymmetric and cross-border threats. As such, they must be confronted at both the national and international levels. No country is immune to cyberterrorism threats, including mine. Slovakia adopted its national strategy to combat terrorism, based on four key pillars, in line with the objectives of the European Union action plan on combating terrorism: prevention, protection, prosecution and response.

The threats posed by major disruptions of critical infrastructure to a country's economy, infrastructure and national security are real. These threats can be classified into three categories: natural, human-caused and accidental or technical threats.

Although reducing the vulnerabilities of critical infrastructure and increasing its resilience is the responsibility of individual States, the need for international cooperation is growing rapidly. As has been mentioned, cyberthreats and attacks are becoming more common, sophisticated and harmful to States as we come to depend more and more on computer communications systems. At present, cyberterrorist attacks are generally considered to pose a relatively low risk to States. But despite the fact that cyberattacks are occurring with greater frequency and intensity around the world, many either go unreported or are underreported, leaving the public with a false sense of security about the threat itself.

While Governments, businesses and individuals are all being targeted on an exponential basis, infrastructure is becoming a target of choice among both individual and State-sponsored cyberattackers, which recognize the value of disrupting what were previously thought of as impenetrable security systems. Many countries around this table have already dealt with these kinds of actions in the recent past. According to Dell's 2015 annual security report, cyberattacks against supervisory control and data-acquisition systems doubled in 2014, to more than 160,000.

Today, according to INTERPOL, malicious code can potentially be used to manipulate the controls of power grids, financial services, energy providers, defence systems, health-care databases and other critical infrastructure, resulting in real-world catastrophic physical damage, such as blackouts or the disruption of an entire city's water supply.

Our joint action is necessary. Some studies suggest that the following measures should be taken to improve critical infrastructure protection: first, assess critical infrastructure vulnerabilities; secondly, develop plans to eliminate significant vulnerabilities; thirdly, propose systems for identifying and preventing attempted major attacks; fourthly, develop plans for alerting, containing and rebuffing attacks in progress; and fifthly, rapidly reconstitute minimum essential capabilities in the aftermath of an attack.

It cannot be excluded that in future the use of cyberspace by State or non-State actors may amount to a threat to international peace and security and will require the Security Council to take more decisive steps to respond.

As stated by the Secretary-General in the foreword to the 2015 report (A/70/174) of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2015:

> "Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be

international law and the principles of the Charter of the United Nations.”

Unfortunately, however, international treaties intended to address the problem have so far had a limited impact because of, first, the inability to hold signatories accountable and, secondly, the difficulty of accurately determining the identity of responsible actors.

Enhanced information-sharing, combined with a mandate to swiftly and accurately release information regarding attacks on impacted citizens, provide a sensible foundation for designing a protocol to effectively address future attacks and may help, yet very few Governments routinely engage in this practice.

The United Nations Global Counter-Terrorism Strategy calls on Member States to improve efforts related to ensuring the security and protection of particularly vulnerable targets and to share best practices, and stresses the importance of developing public-private partnerships in this area. But again so little has been done in practice, as shown by the experience of many countries.

In this respect, I would like to underline the following five points on which we should be concentrating.

There is a need, first, to support States with practical assistance in the implementation of the provisions of the United Nations Global Counter-Terrorism Strategy; secondly, to establish appropriate mechanisms to facilitate the enhanced sharing of best practices; thirdly, to strengthen the capacity of both the public and private sectors and to increase the development of public and private partnerships, including by promoting awareness and understanding of the necessary balance between economic and security interests, in order to ensure an adequate level of protection and limit the detrimental effects of disruption on society and citizens; fourthly, to be more decisive in efforts to combat money-laundering and the financing of terrorism, as it is through this channel that a great deal of know-how falls into the wrong hands; and, fifthly, for the Security Council to consider making better use of the Counter-Terrorism Implementation Task Force Working Group on the Protection of Critical Infrastructure, Including Vulnerable Targets, Internet and Tourism Security. All of this should be aimed at avoiding, addressing and preventing attacks on critical infrastructure such as those that have taken place in recent decades to many countries represented this Chamber and to other Members of the United Nations.

Terrorism poses a threat not only to our security but also to the values, rights and freedoms of our societies and their citizens. My country is committed to playing its part in regional and global efforts to fight terrorism and violent extremism on all fronts, including the protection of critical infrastructure and the sharing of best practices and technologies.

The President: I now give the floor to the representative of Peru.

Mr. Meza-Cuadra (Peru) (*spoke in Spanish*): I should like at the outset to thank the Ukrainian presidency for having convened this open debate of the Security Council on the issue of the protection of critical infrastructure against terrorist attacks. I should like in particular to welcome Mr. Pavlo Klimkin, Minister for Foreign Affairs of Ukraine, who honours us with his presence today. We wish also to thank previous speakers and to welcome the adoption of resolution 2341 (2017).

The protection of critical infrastructure, particularly from attacks by terrorist groups, should be a priority for all States in the framework of the United Nations Global Counter-Terrorism Strategy, with the goal of preserving the health, security and economic well-being of citizens as well as the proper functioning of the State and its administration.

As has been stated, critical infrastructure includes the various facilities, networks and services of the economic and social structure of States, including communication routes, basic services, and tourist and recreational facilities. These should be taken into consideration in the process of designing protection strategies.

Peru having been the target of terrorist attacks in the past, we know that critical infrastructure is a preferred target for terrorist organizations due its vulnerabilities — and all the more so when such attacks lead to serious consequences, such large loss of life and the destruction of property, and, in the medium- and long-term, to economic losses and insecurity among the population.

With the development of information and communication technologies, the Internet and virtual infrastructure have also become a target of attacks for terrorist organizations. The increasing interconnectivity and greater technological dependency increase our vulnerability: the services of an airport control tower,

a nuclear power plant or the valves of a dam can be simultaneously attacked remotely.

In Peru, we are aware of the importance of protecting ourselves against those threats. In 2009, we set up a cybersecurity incident response team, which works closely with the national police and is developing a national cybersecurity network. Faced with global threats there should be global solutions. In that regard, Peru strongly believes in the importance of international cooperation and the exchange of experience and good practices in order to find effective and innovative responses. States must work together while using regional and international coordination mechanisms.

The United Nations plays a key role based on the Global Counter-Terrorism Strategy and its comprehensive, coordinated and balanced implementation across all of its different pillars. We welcome the work of the Working Group on Protecting Critical Infrastructure of the Counter-Terrorism Implementation Task Force. We urge it to coordinate efforts to establish the necessary mechanisms to provide the necessary technical assistance to Member States at their request.

Similarly, my delegation recalls the importance of completing the process of drafting a general convention on international terrorism and of convening a high-level conference on this topic under the auspices of the United Nations. We call on everyone to step up their efforts to conclude such a convention.

I would like to reiterate the commitment of Peru in combating the threats posed by terrorism and violent extremism. To that end, Mr. President, you can count on the constant support of my delegation.

The President: I now give the floor to the representative of Colombia.

Ms. Mejía Vélez (Colombia) (*spoke in Spanish*): I congratulate Ukraine on its assumption of the presidency of the Security Council. I would also like to thank the Chef de Cabinet of the Secretary-General and the representatives of the various entities who shared their points of views this morning on a matter of global concern.

The convening of this debate comes at a time when the frequency and threat of terrorist attacks witnessed around the world is latent in all countries without any distinction. We are confronting new challenges that challenge our capacity for prevention and effective responses.

For Colombia, the protection of critical infrastructure against terrorist attacks has been at the centre of our Government policy. As a result of the internal conflict that affected us for more than 50 years, my country has suffered terrorist acts that have sought to destabilize the functioning of the Government and society. Those attacks or attempted attacks targeted oil infrastructure, telecommunications centres, power grids, transportation, networks for the warehousing of gas and fuel, banking and financial systems, water supply systems and emergency services.

Those attacks forced us to develop within our armed forces the Centres for Special Operations for the Protection of Critical and Economic Infrastructure of the State, which make cooperation possible among communities, the public service and the private sector — the businesses who provide those services — by launching initiatives such as those involving the development of standardized documents and security protocols, which are developed jointly between security agencies and sectors that seek to optimize security in their activities. Fortunately, the peace process will make it possible for those lessons learned to be shared with others and, hopefully, that will be of use to the international community.

As you, Mr. President, emphasized in your concept note (S/2017/104, annex), in my country we have been working with various communities based on trust and dialogue, and, as the Chef de Cabinet and the Secretary-General of INTERPOL mentioned this morning, States must identify vulnerabilities in all possible sectors, strengthen cooperation on prevention and mitigation and ensure greater technical cooperation to enhance the capacities of States, including through the exchange of intelligence, good practices and lessons learned.

For Colombia, acts of terrorism are criminal and unjustifiable, whatever their motivation, wherever they occur and whoever commits them. Terrorism cannot and should not be associated with any religion, civilization, ethnicity or nationality.We reaffirm our commitment to prevent, combat and eliminate terrorism and its financing, in accordance with the principles of the Charter of the United Nations, with full respect for the sovereignty of States, the rule of law and international law.

The President: I now give the floor to the representative of the Islamic Republic of Iran.

Mr. Khoshroo (Islamic Republic of Iran): At the outset, let me express my gratitude to the delegation of Ukraine for organizing this open debate, as well as to thank the briefers for their inputs.

I align myself with the statement delivered by the representative of Venezuela on behalf of the Movement of Non-Aligned Countries.

Today we are facing a proliferation of terrorist acts on an unprecedented scale. No country is immune from the possibility of falling victim to terrorist acts. The most recent terrorist attacks, particularly those committed by Da'esh and other extremists and terrorist groups, serve to show that critical infrastructure is increasingly becoming an attractive target for terrorist operations. The real dimensions of this global menace is revealed when we note the fact that there are still tens of thousands of terrorists, including women and youth from over 100 countries from all the regions of the world, who have joined the rank and file of terrorist organizations. Terrorist acts against critical infrastructure create a state of terror among the general public and inflict adverse consequences on the economic and social development of States, including the possible disruption of the delivery of basic services. Therefore, there is a dire need to protect infrastructure against a growing number of diverse terrorist attacks, both physical and cyber.

Terrorist attacks against infrastructure, such as energy and water supplies, financial institutions, telecommunications, transportation or governmental structures, may well result in civilian fatalities, harm and loss of property on a large scale, disrupt the proper functioning of public services and bring about chaos in societies. They may also cause widespread environmental damage and significantly undermine national resources and capabilities to face its challenges and emergencies.

The protection of critical infrastructure should therefore be seen in the framework of the fight against terrorism, and needs to be incorporated into national plans for countering and preventing terrorism. At the international level, enhanced resilience on the part of the international community to face these threats is also key to curbing the loss of human life and protect the services that are essential for our societies.

The attacks in Turkey, Iraq, Brussels, Afghanistan and some African countries are the most recent terrorist attacks targeting critical infrastructure. At the same time, we should not overlook the fact that the collective punishment of peoples and the brutalization of peoples under foreign occupation — such as the blockade carried out by Israeli regime against Palestinians for decades — also constitute the gravest form of terrorism, depriving consecutive Palestinian generations from their vital infrastructure and natural resources. In places where war continues to be waged, such as Yemen, much of what was already an impoverished civilian infrastructure has been decimated, helping to strengthen terrorism and destabilize the region. In the face of terrorism as a global threat, we must build a stronger collective political will for international counter-terrorism cooperation. At the same time, we emphasize that all efforts to fight terrorism must be conducted in accordance with the purposes and principles of the Charter of the United Nations and international law.

We need robust coherent multilateral mechanisms if we are to respond to terrorism as a common threat to our world. Since there are no simple solutions to complex phenomena such as terrorism, only mechanisms such as these can ensure that our policies are more coherent and coordinated and prevent careless, imprudent or dangerous unilateral action in the name of combating terrorism.

In conclusion, we believe in the centrality of the role of the United Nations and other relevant international and regional organizations to counter-terrorism and conflict-prevention efforts. Their involvement will improve capacity-building and further enhance the effectiveness of the general effort to counter terrorist attacks, including against critical infrastructure, and at the national, regional and international level.

The President: I now give the floor to the representative of India.

Mr. Akbaruddin (India): I would like to thank you, Mr. President, for organizing today's open debate on an issue of increasing significance in an interconnected world. We also appreciate the informative and thoughtful briefings.

Increasingly, the ideas, industries, markets, resources, services and products we share are interconnected as never before, from the way we trade to the way we invest, the way we travel to the way we

eat and, indeed, from the way we think to the way we live. All of these, in one way or another, depend on the growing proliferation of complex and sensitive networks. These interconnections, underpinning the provision of essential societal functions, have created a new kind of vulnerability, giving terrorists the chance to threaten targets that otherwise would perhaps have been unassailable. Such threats serve the purpose of creating disruption on a scale far beyond the immediate area of an attack. They affect the population on a much broader scale. They force the multiple stakeholders providing basic services to be constantly on guard. They therefore not only add to the stress on the stakeholders and their societies, they also raise the cost of the services provided.

Big urban centres such as Mumbai, New York and London have become targets, since any impact on cities that serve as financial hubs can affect a country's economy in multiple ways. The investigations into the heinous terrorist attacks in Mumbai in 2008 revealed the impact that their perpetrators wanted to have on the psyche and economy of the whole of India. The attacks, whose targets included a hospital, a railway station and hotels, were carefully planned and crafted from beyond our borders in order to produce crippling effects not just on daily life in a bustling metropolis but on an entire country of a billion people.

The protection of critical infrastructure is primarily a national responsibility. However, given that many of our technologies and base templates for systems around the world are similar, threats of attacks on an international stock exchange, a major dam, a nuclear power plant, of the possible sabotaging of oil or gas pipelines or airport air-safety systems, or of the potential blocking of an international canal or strait can have much wider implications and complications that extend far beyond national frontiers.

Many recent terrorist attacks have shown that access to information and communications technologies (ICT), and in some cases their manipulation, has been an important enabler. The global nature of such technologies raises the necessity for international vision and coordination on aspects of policy, with the aim of enhancing our capabilities. Despite years of concern about the problem, States have adopted few international instruments addressing issues resulting from threats from cyberspace.

Current international law is not well positioned to support responses to cyber attacks. Security Council decisions that impose binding counter-terrorism obligations do not mention them. With regard to new treaty law, Member States have been negotiating a proposed comprehensive convention on international terrorism since the latter half of the 1990s, the period that corresponds to the rise of worries about terrorist cyber attacks. The offence defined in the draft text may be broad enough to be applicable to cyberattacks, and yet the possibility of terrorist cyberattacks has not been a catalyst for negotiations even after 20 years.

Today's debate is therefore an opportunity to ask ourselves if we can work out our differences in the face of concerns regarding ICT-related threats to critical infrastructure, or if it will require a cataclysmic event to foster greater international collaboration on protecting critical infrastructure from terrorist cyberattacks. Since the threat is discernible and there is understandable global angst about it, can we not look at options for strengthening international law against terrorist cyberattacks? Last month, there was a crescendo of support in this Chamber for a preventive approach. Are we therefore ready for a collaborative preventive approach to addressing terrorist cyberattacks against critical infrastructure? If we are not willing to negotiate a treaty on such attacks, can we at least start by clarifying the applicability of various anti-terrorism treaties to them?

Collaboration is key to moving the perimeter that we defend from our front doors to the edges of our neighbourhoods. Protecting critical infrastructure from terrorist cyberattacks requires a global neighbourhood watch programme because, as the saying goes, there is safety in numbers. Any effective collaboration, however, also requires trust, and right now there is a trust deficit. The lesson of the past is that international law on terrorism has largely developed through States reacting to terrorist violence. We hope that this will not continue to be the case, and the Security Council's adoption today of resolution 2341 (2017) is a first small step in an area where much more needs to be done.

The President: I now give the floor to the representative of Israel.

Mr. Roet (Israel): I would like to congratulate Ukraine and its Minister for Foreign Affairs on its presidency of the Security Council and to wish Ukraine success in the coming month. We thank you,

Mr. President, for convening this timely debate on an important topic, and we were proud to be a sponsor of resolution 2341 (2017), adopted this morning.

For Israel, today's debate is unfortunately not a theoretical one, as we have been coping with terrorist threats since our founding. Today, as terrorism threatens all of us, Israel is in one of the world's most volatile and violent neighbourhoods, threatened from all sides. To the north, we face Hizbullah, which has been designated internationally as a terrorist group, and which hides its arsenal of more than 150,000 rockets, all pointing towards Israel, in civilian homes, schools and hospitals. In threatening civilians from within its own population, Hizbullah is committing a double war crime, and yet its actions are rarely if ever condemned in this Chamber. In 2016, Hassan Nasrallah, Secretary General of Hizbullah, threatened a catastrophic attack on Haifa's ammonia-storage tanks that would, he said, lead to the death of tens of thousands of residents and affect 800,000 Israelis. He went on to declare that this would be exactly like a nuclear bomb and that therefore he could say that today Lebanon had a nuclear bomb.

In the south, we face Hamas, the terrorist group controlling Gaza that openly calls for the destruction of the State of Israel. Hamas also intentionally targets civilians among its own population, while making an effort to target crucial infrastructure. We witnessed that in 2014 when Hamas attempted to paralyse Israel by attacking Ben Gurion Airport, Israel's primary international transport hub.

Israel has previously stated here in the Chamber that wherever there is terror, there Iran is also. Therefore, hearing the statement made by the representative of Iran a few minutes ago reminds me of someone who killed his own parents and then begs the mercy of the court because he is an orphan. Iran is the leading State sponsor of terror, backing and supporting the operations and activities of Hizbullah, Hamas and other terror groups based in the Middle East and throughout the world.

Iran continues to test increasingly advanced ballistic missiles, in a direct threat to Israel. Just last week, on 4 February, a senior member of the Iranian Parliament's National Security and Foreign Policy Commission stated, "only seven minutes are needed for the Iranian missile to hit Tel-Aviv". The test firing of that ballistic missile proves once again that Iran is ignoring resolution 2231 (2015). I call upon the Security Council to respond firmly and decisively to such Iranian violations and provocations.

We have recently witnessed a wave of terror attacks on critical infrastructure across the globe, including by Da'esh. The downing of the EgyptAir jetliner aircraft over the Mediterranean Sea, the attacks in Istanbul's Ataturk Airport, and the Brussels metro station and airport bombings left hundreds dead and wounded, proving once again that no country is safe and no person is immune to such despicable attacks.

From global transportation to financial systems, from energy infrastructure to water supplies, attacks on critical infrastructure threaten the very foundations on which our modern society is built. Terrorists recognize that perpetrating attacks against critical infrastructure has the potential for devastation that transcends the target itself. Attacks on major infrastructure networks have the ability to paralyse the workings of entire countries and regions.

We must adapt every day to the constant and evolving terror threats that aim to attack our infrastructure, our civilians and our citizens. We recognize that the only way to combat such threats is by staying ahead of the game, remaining vigilant and anticipating the next step of the perpetrators. Today's realities require us to address not only physical attacks. We are now fighting on a whole new front, and we must also guard against cyberthreats and attacks.

Critical infrastructure is closely linked to technology and the associated danger of cyberattacks. Cyberattacks have no borders and are not limited to State actors. Perpetrators meet no physical barriers and can cause even greater damage than a physical terror attack on a single location. Through Israel's high-tech security culture and joint private-public cyberventures, Israel has successfully combated threats that impact both private and State systems.

It is said that necessity is the mother of invention. Out of necessity, we have become experts in the field of counter-terrorism and are proudly sharing our knowledge with Governments throughout the world. Israeli experts are contributing their expertise on a wide range of issues — from terrorist financing to forensic investigation and from aviation security to border protection. Those activities reflect our fundamental belief that terrorism can be effectively confronted only through international cooperation. A serious international threat requires a serious international

response. We are committed to taking all necessary steps to continue protecting our citizens and sharing our knowledge with the international community.

The President: I now give the floor to His Excellency Mr. Vale de Almeida, Head of the Delegation of the European Union to the United Nations.

Mr. Vale de Almeida: It is my honour speak on behalf of the European Union (EU) and its 28 member States.

The candidate countries of the former Yugoslav Republic of Macedonia, Montenegro, Serbia and Albania; the country taking part in the Stabilization and Association Process and potential candidate Bosnia and Herzegovina; as well as Ukraine and the Republic of Moldova and Armenia, align themselves with this statement.

Let me first congratulate Ukraine on its current presidency of the Security Council and to thank Sweden for its excellent presidency last month. I would like to commend Ukraine for organizing today's debate and for this opportunity to speak about the protection of critical infrastructure, a topic of major concern for the European Union and its member States. I would also like to stress the importance of working together on this issue at the international level to ensure a high degree of protection of our critical infrastructure and to increase their resilience to terrorist attacks and other disruptions.

The questions raised in the concept note (S/2017/104, annex) are very important.I would like to address them briefly, one by one.

On the first question, about our tools, in Europe we have in place the European Programme for Critical Infrastructure Protection. In place since 2006, it sets the overall framework for activities aimed at improving the protection of critical infrastructure in the European Union across all relevant sectors of economic activity. The programme aims to respond not only to terrorist threats, but also include man-made, technological threats and natural disasters. In short, it seeks to provide an all-hazards cross-sectoral approach. The programme is supported by regular exchanges of information between EU member States in the framework of the meetings of the critical infrastructure protection contact points.

A key pillar of the programme is the 2008 European critical infrastructures directive, which establishes a procedure for identifying and designating European critical infrastructures and a common approach for assessing the need to improve their protection. Those refer to critical infrastructure located in member States whose disruption or destruction would have a significant impact on at least two member States. It has a sectoral scope and applies to the energy and transport sectors.

The directive furthermore requires owners and operators of designated European critical infrastructures to prepare operator security plans — advanced business continuity plans — and nominate security liaison officers, linking the owner/operator with the national authority responsible for critical infrastructure protection. The application of the directive is monitored by contact points appointed from each EU member State. The contact points group also engages with the European Commission in international cooperation outside of the EU — so far with United States of America and Canada — but, this year, will also start to engage with neighbouring countries in Eastern Europe and the Balkans.

Reacting to new threat developments, in 2016 the EU adopted a joint framework to counter hybrid threats, which also covers the matter of the protection of critical infrastructure against hybrid and asymmetrical threats, such as in the field of energy and transport. It is designed to strengthen member States' resilience in that area and foresees cooperation with EU partners in countering such threats.

With regard to the second question, on methods to promote improved responsiveness to terrorist attacks and the resilience of critical infrastructure, the European Commission has funded over 120 different projects under the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme between 2007 and 2013. That programme was designed to protect citizens and critical infrastructures from terrorist attacks and other security incidents by fostering prevention and preparedness, improving the protection of such infrastructure and addressing crisis management. A key objective was to provide expert knowledge and the scientific basis for better understanding criticalities and interdependencies. The increase in cyberthreats also led the EU to adopt legislation on the security of network and information systems in July 2016.

As for the third point, on how to strengthen the capacity of both the public and private sectors to prevent attacks and react to threats to critical infrastructure, training sessions and exercises have been very useful

tools, which the European Union has encouraged and engaged in. A good example is the VITEX 2016 exercise, which was designed and coordinated by the Dutch presidency of the European Union. It was the first EU-wide exercise focusing on the effects of large-scale failure of critical infrastructure — in this case electricity — across Europe. The VITEX 2016 exercise resulted in an exercise guide with an exercise design, which describes step-by-step how such an exercise can be organized. This guide is available to everyone in order to encourage possible follow-up exercises in the future.

Addressing the fourth point on mechanisms and platforms for cooperation, I want to point to the vital importance of regular exchanges of information and best practices. The European Commission has for such purposes developed the Critical Infrastructure Warning Information Network, which is an Internet-based, multi-level system for exchanging critical infrastructure protection ideas, studies and good practices among Member States and key stakeholders. This portal, which has been operational since mid-January 2013, also seeks to raise awareness and contribute to the protection of critical infrastructure in Europe.

As for my last point — the role of the United Nations and its agencies in this work — there is certainly a potential for further cooperation as the security and protection of critical infrastructure are a concern we all face, as is the fight against terrorism. The European Union would be interested in cooperating internationally, with partners beyond its border, in the area of protection of critical infrastructure against this common threat. We are already engaged in various forums, such as the Organization for Security and Cooperation in Europe and the Council of Europe, but would also welcome United Nations initiatives in this field, and we stand ready to explore possibilities for such cooperation.

The President: I give the floor to the representative of Romania.

Mr. Jinga (Romania) (*spoke in French*): I would like to thank the Ukrainian presidency of the Security Council for its initiative of placing the protection of critical infrastructure against terrorist attacks on its agenda for the first time. I also thank the briefers who, through their interventions, have enriched this open debate.

Romania fully endorses the statement of the European Union. I should like to add a few remarks from my national perspective.

Transport, telecommunications, energy or water distribution networks, financial systems and emergency services infrastructure — what is called critical infrastructure — is essential to the sound functioning of our contemporary society. Consequently, their protection is a key priority. Terrorist entities have demonstrated the ability to act with tenacity, speed and flexibility. Given their goal of producing the greatest number of casualties and material damage, critical infrastructure remains a preferred target.

The global dimension of terrorist threats and attacks requires a comprehensive response, and the United Nations must play a key role in a coordinated and effective approach. Given the inter-State connections of critical infrastructure, regional and global cooperation is also crucial. In recent years, terrorist attacks on critical infrastructure have highlighted the vulnerability of States. We all remember the most recent cases, which demonstrated the impact of the terrorist attacks on the Brussels and Istanbul airports. We must not forget the most deadly attacks in the history of Spain against passenger trains in Madrid in 2004.

In addition, the international community has witnessed the horrors committed against civilians in Syria, where water became a weapon of war when more than 5 million inhabitants of the capital were deprived of water for more than a month after an attack against its main supplier of water. We also recall the destruction in 2013 of the Deir ez-Zor suspension bridge on the Euphrates, cutting access to around 50,000 people in the city, or the Da'esh attacks that targeted oil wells, refineries and power stations in Syria and Iraq. Unfortunately, the list is not exhaustive. No State is completely immune.

In 2011, Romania developed a national strategy for the protection of critical infrastructure. We believe that in our efforts to protect critical infrastructure, we must place greater emphasis on cooperation among State authorities, economic operators and the public, as well as on risk analysis and the operationalization of the public-private partnership. The latter is essential, since a significant portion of the infrastructure belongs to private or multinational companies.

Among the means that terrorist entities exploit of and that offer immense opportunities are computer

technologies and online communication, which have exhibited unprecedented growth. Experience has shown that the most serious terrorist threats are of a mixed nature, enabling cyberattacks to have a direct impact on physical infrastructure. In that context, prevention has become increasingly significant.

In 2013, Romania adopted a cybersecurity strategy and a national action plan for the implementation of its national cybersecurity system. Moreover, in 2011, Romania set up the National Cybersecurity Incident Response Centre, tasked with public prevention, response and advisory services. Currently, the Centre is implementing a project in conjunction with partners from 27 organizations, from 14 European countries.

Another effective means of combating terrorism is the prevention of violent extremism, in which Romania has also invested heavily, with results that speak for themselves. My country has not experienced the phenomenon of foreign terrorist fighters or seen a single case of a Romanian citizen or foreign national travelling to the theatre of war to join a terrorist organization. Furthermore, in Romania, jihadi propaganda is found only in extremely isolated pockets.

We deeply appreciate United Nations efforts to develop legal and institutional frameworks for the fight against terrorist threats to be placed at the disposal of the Member States. Romania was a sponsor of resolution 2341 (2017), on the protection of critical infrastructure from terrorist attacks, adopted unanimously today by the Council. It complements the adoption of resolutions 2322 (2016), on international judicial cooperation; 2309 (2016), on combatting threats to civil aviation; and resolution 2286 (2016), on the protection of personnel and medical facilities in armed conflicts. Another important pillar remains General Assembly resolution 71/19, on cooperation between the United Nations and the International Criminal Police Organization, INTERPOL.

We welcome the decision of the Secretary-General to launch a thorough debate on the implementation of the Organization's Global Counter-Terrorism Strategy. The informal discussion, to be held in the General Assembly, thus represents a good starting point for strengthening the United Nations' counter-terrorism component.

In conclusion, Romania believes that the respect for international legal frameworks and the adoption and implementation of national laws are essential to any effort to protect critical infrastructure from terrorist attacks.

The President (*spoke in French*): I give the floor to the representative of Belgium.

Mr. Buffin (Belgium) (*spoke in French*): We thank the Ukrainian presidency of the Security Council for having convened this public debate on the important topic of the protection of critical infrastructure from terrorist attacks. We also thank the briefers for their statements.

Belgium fully aligns itself with the statement delivered by the observer of the European Union.

Multiple responses are needed to counter terrorism and violent extremism. First, we must tackle the root causes of the phenomenon by collectively protecting our fundamental values: respect for human rights, the rule of law, good governance, sustainable development, the fight against impunity and the promotion of tolerance. The international community must also join forces to promote the peaceful and political resolution of the far too many conflicts ravaging our planet.

In that connection, Syria is the clearest tragic example, but is unfortunately not the only conflict. Other regions are embroiled in war and instability that are conducive to the growing influence of terrorist groups. In that regard, we highlight the Security Council's particular responsibility to unite the international community in efforts to find peaceful and political resolutions to those conflicts. Additionally, it is clear that we must directly confront Da'esh, Al-Qaida and affiliated groups. In that regard, Belgium is an active participant in the international coalition against Da'esh.

With particular regard to the protection of critical infrastructure, I would like to make the following comments. In this area, as in others, the importance of prevention is paramount. In that respect, modern methods of prevention, based on adequate training of security officers and law enforcement officials, should be developed. Belgium attaches great importance to these aspects, in particular through the organization of drills and the introduction of specific training programmes for its security forces.

The critical infrastructure security plan must contain both physical measures, such as the installation of security barriers or surveillance cameras, as well as cybermeasures such as firewalls or detection systems. In addition, authorities should ensure the development

of digital emergency planning, and crisis and alert management for populations directly affected by an emergency. In Belgium, for example, the Belgian Centre for Cyber Security, created in 2014, has developed a national plan that describes the roles and tasks of the various authorities in the event of a national incident or national cyber security crisis.

Effective public-private cooperation is another important area of prevention and response to threats, as it is not uncommon for parts of critical infrastructure to belong to the private sector. There is therefore a need to increase opportunities for the public and private sectors to meet, in particular through conferences, drills or trainings. Establishing an information network among private companies and public authorities against terrorist threats is an extremely important tool in that respect.

Strengthening international cooperation, including through information exchange, joint drills and the development of scenarios and contingency plans, should be encouraged. With this in view, the European Union (EU) has developed, together with its member States, a number of tools to deal with the threat, notably the European Programme for Critical Infrastructure Protection and the European Directive of 6 July 2016 on network security and information systems within the EU. Because those tools, as well as others, were detailed in the statement made by the representative of the EU, I will not revisit them.

The important role of the United Nations, in particular through the Counter-Terrorism Committee, the Executive Directorate — which assists the Committee — and the Counter-Terrorism Implementation Task Force, bears mentioning. These bodies can work usefully to raise Member State awareness on the issue of protecting critical infrastructure against the terrorist threat by promoting the exchange of good practices in the operational framework. Such awareness-raising may include, for example, the organization of meetings in which States share lessons learned from their own experience and present best practices that have proven successful. The United Nations is a vital forum for developing the exchange of information and best practices and helping to identify gaps in the protection of critical infrastructure. For that reason, Belgium sponsored resolution 2341 (2017) adopted at the beginning of this meeting.

The President: I now give the floor to the representative of Argentina.

Mr. Garcia Moritán (Argentina) (*spoke in Spanish*): At the outset, I should like to thank the Ukrainian presidency for the invitation to participate in this open debate on an issue of such importance to the international community.

Argentina condemns terrorism in all its forms and manifestations and considers that terrorist acts not only constitute a threat to international peace and security, but are also a threat to human dignity, peaceful and civilized coexistence, stability, the consolidation of democracy, and the economic and social development of nations. Our country, which was the victim of bloody terrorist attacks in the 1990s, reiterates that terrorist acts are criminal and unjustifiable, whatever their motivation and wherever and by whomsoever they are committed.

Terrorism cannot be tackled solely through the enforcement of defence or security measures. Instead, a comprehensive approach should be taken — such as that reflected in the United Nations Global Counter-Terrorism Strategy — based on the balanced implementation of the four pillars of the strategy, within the unrestricted respect for international law, international human rights law, international humanitarian law and international refugee law.

Critical infrastructure are those that are indispensable for the proper functioning of essential services for society: health, security, defence, the social and economic well-being of citizens and for the effective functioning of the State, whose total or partial destruction or disruption affects or significantly impacts those services. We therefore welcome the approach chosen for this debate, due to the urgency of the threat posed by terrorism to the vital services and infrastructure of our countries. In that regard, there is a need for greater cooperation, coordination and information exchange among agencies and organizations within each country, as well as among the various countries. There is also a need to adapt to the changing nature of the terrorist threat, physical and cybernetic.

We welcome resolution 2341 (2017), which the Council adopted this morning and which is the first to focus specifically on the issue of the protection of critical infrastructure. We agree on the need to call on States to develop and improve their strategies for risk

assessment and risk reduction and to cooperate in this regard. Collaboration between the public and private sectors in this area is also key to mitigating risk and preventing attacks on this type of infrastructure.

Aware of the importance of addressing this problem without delay, our authorities have set up a working group within the Ministry of Modernization to draw up guidelines for an action plan for the identification and development of regulations and measures for the protection of critical infrastructure, including information infrastructure. The working group should determine the criteria for identifying infrastructure, the sectors involved, and the regulatory bodies and companies or organizations responsible. The group will also develop a working methodology to carry out a risk assessment and establish measures to manage those risks. An inter-institutional approach involving all relevant sectors will be taken.

With respect to cybersecurity, we are of the view that achieving adequate levels of security in the digital universe is essential for information and communication technologies (ICTs) to reach their full potential. A strong commitment from the international community is required to avoid and limit the misuse of technological tools by various State and non-State actors. We must take into account, however, that there is a broad spectrum of non-State actors that carry out network security attacks using ICTs. Those actors range from terrorist groups and transnational criminal organizations to individual offenders. Responses to these threats require specific and separate international legal instruments to articulate effective international cooperation systems in the prevention, prosecution and criminal repression of such conduct.

Finally, we reaffirm the central role of the United Nations in the fight against terrorism, as the pillar of the multilateral system of universal composition,and having the primary responsibility for the maintenance of international peace and security. We are convinced that multilateral action, through the United Nations, in accordance with the principles of the Organization, will enable us to address the threat of terrorism in full respect for international human rights law and international humanitarian law, and to achieve a more secure world for all.

The President: I now give the floor to the Permanent Observer of the Observer State of the Holy See to the United Nations.

Archbishop Auza (Holy See): The open-ended litany of terrorist attacks in cities and villages continues to remind us of the threat of terrorist attacks to civilian infrastructure and to civilian populations. This wave of terror, which considers innocent civilians as legitimate targets of violence, either directly or indirectly, through the destruction of the civil infrastructure on which we depend, must be counteracted by the actions by a unified international community.

Recent conflicts in the area of ancient Mesopotamia have had a devastating impact on ancient ethnic, religious and cultural minorities that for millenniums have inhabited the region. Parties to those conflicts have purposefully sought to destroy the cultural fabric and the historical rootedness of those communities in the region by destroying their religious and cultural heritage sites. The intentional destruction of the infrastructure critical to the survival of those communities, such as schools, hospitals, water supplies and places of worship, has become a strategy to annihilate them collectively, immiserating and eradicating them by attacking the structures that give them a modicum of communal existence.

It is the obligation of the international community, in accordance with the Charter of the United Nations, to protect civilians and their critical infrastructure from the brutality and barbarity of terrorist groups. Part of that obligation is to heighten public awareness of that terrorist tactic and to urge States to maintain a high level of critical infrastructure protection and resilience, as well as public preparedness, in the event of an attack, and to prevent, as much as possible, the disruption of critical services and the loss of human life. My delegation therefore believes that this debate is a response to such a need.

More effective and lasting measures to protect critical infrastructure against terrorist attacks must be based on policies that reject the unfettered pursuit of profit and narrow geopolitical interests, even at the cost of the destruction of critical civil infrastructure. In that regard, my delegation wishes to reiterate the Holy See's appeal to weapon-producing nations to severely limit and control the manufacture and sale of weapons, ammunition and technologies to unstable countries and regions of the world, where the likelihood of their illegal use or their falling into the hands of non-State actors remain a real and present danger.

The international community must also address the role of organized crime in the sale or barter of weapons capable of destroying critical infrastructure. States should be urged to collaborate in that area, at both the international and the regional levels, through the sharing of information and best practices, coordinated policies and joint border controls.

The world must act to prevent terrorists from having access to financial support from terror sponsors. The borderless nature of the terrorist groups perpetrating the destruction of critical infrastructure requires the international community to control the cybertechnologies that violent groups use to recruit new adherents, finance their activities and coordinate terrorist attacks.

Pope Francis has spoken on a number of occasions of our age as a time of war, namely, a third world war that is being fought piecemeal, one in which we daily witness savage crimes, brutal massacres and senseless destruction, like the destruction of infrastructure critical to the existence of entire populations.

The international community must come together as one to put an end to this war fought piecemeal. Such unity is necessary if the international community is going to achieve the shared objective of protecting critical infrastructure against terrorist attacks. Our common goal will be achieved most quickly and effectively through an unselfish sharing of critical information and best practices and of resources and technologies among States, in particular with those States that are the least capable of protecting their critical infrastructure and populations from terrorist attacks.

The President: I now give the floor to the representative of Turkey.

Mr. Begeç (Turkey): At the outset, I would like to thank Ukraine for organizing this open debate, a follow-up to the very useful Arria Formula meeting held in November. I also wish to thank the speakers for their briefings. Turkey welcomes the adoption of resolution 2341 (2017), which it co-sponsored.

At the forefront of the fight against terrorism, Turkey is currently fighting several terrorist organizations simultaneously, We know only too well the deep suffering, damage and loss of life caused to individuals, families and society. More than 500 innocent lives were lost and many more wounded owing to terrorist attacks by Da'esh and the Kurdish Workers Party (PKK) during the past year and a half.

Terrorist organizations are very aware of the potential damage that the attacks on critical infrastructure can cause. Terrorist attacks targeting critical infrastructure, including sectors such as the energy, transport, telecommunications, defence and chemical industries, not only cause human and material loss, but they also carry the potential to disrupt public safety and the delivery of key public services, thereby affecting the functioning and well-being of societies, as pointed out in the President's concept note (S/2017/104, annex).

Turkey is indeed a victim of such attacks. In June 2016, Da'esh targeted the Istanbul Atatürk Airport, while the PKK has attacked water dams, pipelines, health services and public and private institutions, including schools, education facilities and medical infrastructure. The PKK has also kidnapped civil servants, including health, education and customs personnel. Moreover, State institutions, including the Turkish Parliament, were bombed by the Fethullah Terrorist Organization during the foiled coup attempt of 15 July 2016.

Faced with the serious threats posed by multiple terrorist organizations, Turkey has taken certain measures to protect the lives of its people, as well as public and private institutions and investments. Turkey attaches particular importance to the security of critical energy infrastructure, owing to the country's increasing energy demands as a result of its ever-growing economy as well as its geostrategic position, which provides a sustainable route between producer regions and consumers. One measure that we took and found useful was the establishment of committees for the security of critical energy infrastructure and for pipeline security, under the Ministry of Energy and Natural Resources.

The protection of critical infrastructure from terrorist attacks is a complex issue, involving both public and private sectors and requiring the protection of cross-border infrastructure and international preparedness. International cooperation and the sharing of best practices are therefore needed. That is why many international and regional organizations, including NATO, the Organization for Security and Cooperation in Europe and the European Union, have been focusing on the issue.

As a country that attaches importance to the centrality of the work of the United Nations in global counter-terrorism efforts, we note that the protection of critical infrastructure was also one of the goals included in the United Nations Global Counter-Terrorism Strategy, adopted in 2006. We thank the Chef de Cabinet of the Secretary-General for an overview of the work of the United Nations on that issue. We hope that the United Nations will pursue further its efforts to that end in close coordination with other international and regional organizations dealing with the matter.

In that connection, I would also like to mention the importance of protecting soft targets, which include religious centres, tourist sites and public surface transportation facilities, as well as business and commercial facilities, such as hotels, restaurants, stadiums and entertainment venues, where people come together and which are relatively vulnerable to terrorist attacks owing to their open access and limited security. Concerns about protecting soft targets are not new. However, terrorist groups increasingly target such venues, as we have seen in the terrorist attacks perpetrated in Istanbul near a football stadium in December 2016 and in a night club on 1 January 2017, which claimed the lives of many Turkish and foreign nationals.

In that regard, the inaugural meeting of the "Protection of Soft Targets in a Counterterrorism Context Initiative", co-led by the United States and Turkey under the auspices of the Global Counterterrorism Forum, was held in Antalya, Turkey, in December 2016. We hope that the set of good practices to enhance the security and resilience of sites that are potential soft targets, which is to be developed within the framework of the initiative as a result of region-specific workshops to be held throughout 2017, can serve as the basis for international engagement, assistance and training so as to enhance the security and resilience of sites that are potential soft targets.

As I emphasized, the protection of critical infrastructure from terrorist attacks is a challenge that we need to confront together. International cooperation is vital. We support the work being done in that area in international and regional organizations. We believe that the United Nations and its agencies have a special role to play in that regard. We stand ready to support any initiatives that could be taken to that end.

The President: I now give the floor to the representative of Cuba.

Mrs. Rodríguez Camejo (Cuba) (*spoke in Spanish*): Cuba aligns itself with the statement to be delivered by the representative of Venezuela on behalf of the Non-Aligned Movement.

Our country reiterates its unwavering willingness to combat terrorism and expresses its categorical rejection and condemnation of all terrorist acts, methods and practices in all their forms and manifestations, irrespective of motivations, including State-sponsored terrorism. Cuba, in compliance with the 18 international conventions pertaining to terrorism to which it is a State party, has carried out relevant legal measures, such as law 93 on acts of terrorism. The Cuban people bear the scars of terrorist acts organized, financed and executed from abroad which have resulted in a toll of 3,478 dead and 2,099 disabled.

The Cuban Government has never allowed, nor will it ever allow, the use of its national territory to carry out, plan, support, conceal or finance acts of terrorism targeting any other State, without exception. Our country supports the adoption of a general convention on terrorism and favours the convening of an international conference, under the auspices of the United Nations, that would allow us to reach a multilaterally agreed response to terrorism. We reject and condemn the double standards and selectivity in the treatment of this issue. Combatting terrorism cannot be used as a pretext for interference, interventionism, aggression or violations of international and human rights law.

We call for an end to the financing, equipping, training of, supplying of arms and support of any kind to terrorist groups in all their forms. In the light of the militarization of cyberspace and the proliferation of cybercrime and cyberterrorism, it is increasingly urgent for States to ensure that information and communication technology, the Internet, television, radio and other parts of their critical infrastructure are not used by terrorist groups.

As a result of growing interconnectivity, critical information infrastructure is now exposed to an increasing and more varied number of threats and weaknesses, which pose new security challenges. The use by State and non-State actors of new information and communication technologies for purposes incompatible with international peace and security is a serious problem, which requires efforts by all States.

The undercover and illegal use by individuals, organizations and States of the information systems of other nations in order to attack third countries has the potential to trigger serious conflicts. The only way to prevent and address these threats is through joint cooperation among all States to ensure cybersecurity and to protect critical infrastructure by supporting national efforts aimed at strengthening human capacity, creating more learning and employment opportunities, and improving public services and the quality of life of the population. We must achieve a legally binding international instrument, within the United Nations system, that regulates the use of information and communications technology and ensures that it is only used in accordance with international law and in particular with the Charter of the United Nations.

The President: I now give the floor to the representative of Iraq.

Mr. Alhakim (Iraq) (*spoke in Arabic*): At the outset, allow me to thank Ukraine and its Minister for Foreign Affairs for convening this important open debate on the protection of critical infrastructure. Iraq also welcomes today's adoption of resolution 2341 (2017) , which Iraq co-sponsored.

We must not attribute terrorism to any religion, culture, nationality or geographical region, as affirmed by numerous Security Council resolutions, the most recent of which being resolution 2253 (2015). The challenges represented by terrorist organizations, such as the Islamic State of Iraq and the Sham (ISIS) terrorist gangs, emanate from their high organizational capacity, which allows them to perpetrate terrorist attacks in cyberspace that have a direct physical impact on critical infrastructure. The attacks destroy and impede the functionality of critical infrastructure and cause serious damage. ISIS gangs are working to strengthen their organizational capacities and strategies aimed at recruiting supporters from developed nations who have received an education in prestigious Western universities. These highly educated recruits allow terrorist organizations to carry out transborder cyberattacks that evade all national restrictions, thereby creating a reality in which there are in fact no borders.

Strengthening international cooperation in the area of counter-terrorism is extremely important, in particular because ISIS perpetrates its crimes through decentralized networks. These gangs have increased their technical capacities for the purpose of carrying out cyber attacks and have recruited foreign terrorists who have advanced skills to carry out such complex attacks.

Among the most important trends that can be observed in the conduct of terrorist organizations, in particular of Da'esh terrorist gangs, is the continued targeting of critical infrastructure in Iraq, including bridges, power lines, telecommunications towers and oil pipelines. Terrorism has impacted many projects that constitute the backbone of Iraq's infrastructure. Terrorists have also burned monuments, mosques and universities. Such terrorist attacks have increased the cost of development projects because of the growing cost of security measures necessary to protect construction sites. The targeting of oil facilities and refineries in Iraq in areas that witness many terrorist attacks is one of the most serious attacks on Iraq's economy and infrastructure because the country depends primarily on revenue from oil.

The liberation of Iraqi cities that were previously controlled by Da'esh gangs usually comes at great economic cost. In the battle to reclaim Mosul, ISIS gangs planted mines and explosive devices in citizens' homes and in public buildings and on bridges to destroy them and prevent security forces from advancing towards these cities and towns. These challenges have grown as oil prices have fallen on the global market, since petroleum revenues form the core of Iraq's national budget.

In conclusion, my Government is deeply grateful for the active role and efforts of the global coalition, the United Nations Assistance Mission for Iraq and other international organizations, particularly the United Nations Development Programme. We call on the international community to make further efforts to reconstruct the liberated areas of my country, restore stability and rehabilitate our infrastructure, including schools and hospitals.

The President: I give the floor to the representative of Bangladesh.

Mr. Bin Momen (Bangladesh): We thank the Ukrainian presidency for organizing this open debate and the briefers for their insights.

Bangladesh aligns itself with the statement to be delivered by the representative of the Bolivarian Republic of Venezuela on behalf of the Non-Aligned Movement.

Resolution 2341 (2017), adopted today, will help to create further impetus towards protecting critical

infrastructure from terrorist attacks. The resolution comes at a time when there have been reports of terrorists making increasing and sophisticated attempts to find access to and attack critical infrastructure. The need to conduct security analyses for critical infrastructure has become all the more important to enhancing resilience and preparedness in the wake of some recent terrorist attacks in international airports and the targeting of other critical infrastructure.

Today's open debate has been useful in highlighting a number of ongoing national and regional initiatives, especially in the context of growing interdependencies among critical infrastructure sectors. We take note of the work being carried out in different critical infrastructure sectors, including industry and supply-chain management, civic amenities, cross-border transportation and the cybersphere. Such work should form a useful repository of good practices and help to inform further legislative work that remains to be done at the international level, particularly on cybersecurity. The environmental consequences of terrorist attacks on critical infrastructure, especially in densely populated city centres, underscore the complexity of the challenges before us.

In Bangladesh, our authorities concerned shall continue to further study resolution 2341 (2017) in order to identify existing gaps, challenges and strengths at the national level in terms of addressing the possible vulnerabilities of our critical infrastructure to terrorist attacks. We remain mindful of the overwhelmingly transnational nature of most threats to critical infrastructure, and open to strengthening regional and subregional cooperation to that effect. In the areas of our evident capacity constraints, many Member States in a comparable situation will continue to rely on the United Nations as both a first responder and a consistent provider of capacity-building assistance, including for contingency measures.

In the context of building our national-level preparedness, we have been working with the Counter-Terrorism Implementation Task Force and various relevant United Nations entities in the areas of nuclear security, maritime and aviation security, combating the financing of terrorism, and cybersecurity. Such capacity-building work has been critical in terms of making our concerned agencies and other stakeholders better aware of the existing international legal and normative frameworks. They have also helped to conduct mapping of the various mutually reinforcing strands of work by different entities that may benefit from further coordination and coherence. We look forward to drawing upon such work towards developing a national strategic approach to pre-empting and preventing terrorist attacks and threats against critical infrastructure. The work done to protect infrastructure from criminal acts and natural hazards should also contribute to these efforts.

The primacy of risk assessment, early warning and information-sharing in the protection of critical infrastructure and civilians need not be overemphasized. Bangladesh remains a reliable partner of the international community in the area of information-sharing, in conformity with our Prime Minister's zero-tolerance approach to terrorism in all forms and manifestations. We urge the Counter-Terrorism Committee, including its Executive Directorate, to undertake consultations with national and regional actors, while taking stock of Member States' efforts, with a view to drawing on evidence-based, substantiated information.

The critical importance of forging partnerships between the public and private sectors has been underlined by almost all delegations. Bangladesh is keen to participate in and learn from relevant international and regional forums bringing together representatives from the public and private sectors to promote synergistic approaches through their work. We acknowledge the potential merit of further developing certain international emergency-preparedness standards that the private sector may be required to comply with.

Against the backdrop of rapidly evolving terrorist threats, we underscore the need to facilitate knowledge-sharing and technology transfers in the spirit of effective international cooperation and partnership. While all Member States must continue to assume their primary responsibility to address terrorist threats to major infrastructure, much of our collective success will critically hinge on the need-based support to be made available to developing and least developed countries by the concerned development partners, including the United Nations.

The President: I now give the floor to the representative of Pakistan.

Ms. Lodhi (Pakistan): Let me start by thanking the delegation of Ukraine for convening today's debate on such an important issue.

Among the myriad threats endangering global security, terrorism has emerged as one of the most complex and imposing challenges of our times. Our dependence on critical infrastructure makes this an attractive target for terrorists of all stripes. Terrorist attacks on infrastructure aim to disrupt life, cause widespread fear and chaos, retard socioeconomic development and impede regional economic cooperation. Advances in the world of communications technologies, making the world interdependent as well as interconnected, and the increasing use of encrypted communications by terrorist organizations like Da'esh have amplified the threat of a terrorist attack on financial and energy hubs. National resolve and collective endeavour are necessary to protect the infrastructure that is essential to the welfare and progress of our peoples.

My country has confronted and combatted terrorism over several decades with courage and conviction. Our resilience has been tested time and time again, from the barbaric attack on the Marriott Hotel in Islamabad in 2008 to the destruction of military equipment in the attack on an air force base in Kamra in 2012 and the attack on Karachi airport in 2014. These attacks were aimed at destroying and disrupting the lives of my people, weakening our defence forces and demoralizing the nation, but they only strengthened the resolve of our people to continue their efforts to eliminate this scourge.

Over the past four years, Pakistan has adopted a multipronged strategy. A military-led operation called Zarb-e-Azb has successfully destroyed terrorist infrastructure, and a national action plan — undergirded by a strong national consensus — has effectively sought to counter the narrative of terrorist and extremist organizations. That comprehensive approach has succeeded in expelling terrorist organizations from our territory and greatly constrained their ability to carry out lethal attacks, as evident from the dramatic decline in the number of such attacks, despite this morning's cowardly terrorist attack in Lahore. What Pakistan continues to face today are increasingly and externally supported terrorists. One of their principal targets is the major infrastructure that we are currently building in Pakistan. Their aim is to undermine our economic accomplishments and stability.

State control of infrastructure systems and its role in determining how to effectively protect infrastructure are critical. The diversity of the threat requires a coherent response by all national stakeholders based on the specific environment of each individual country. International and regional organizations and regional cooperation also remain vital in countering the threat of terrorism. At the regional level, the sharing of information and threat assessments, as well as effective border management and the sharing of best practices, can significantly enhance national capacities to deter and defeat terrorism.

It was in that spirit that my country joined the Regional Convention on Suppression of Terrorism of the South Asian Association for Regional Cooperation (SAARC). However, unfortunately, SAARC as an organization has become a victim of the hostile agenda of some of our neighbours, which has severely hampered the ability of our region to respond to the multiple challenges it faces, including the challenge of terrorism. Although we remain committed to strengthening regional cooperation to combat terrorism, Pakistan continues to suffer from regional terrorist attacks that are supported by forces within the region. We are determined to repel, and are fully capable of repelling, such State-sponsored terrorism.

The United Nations can, and should, play a role in enhancing Member States' capacities in their counter-terrorism efforts. The Working Group on the Protection of Critical Infrastructure of the Counter-Terrorism Implementation Task Force is playing a positive role in that regard. The United Nations also provides a platform for assisting Member States in identifying potential facilities-related threats and risks and in developing sound strategies and partnerships to implement those plans.

In addressing the terrorist threat, it is essential for the global community to analyse and understand the phenomenon of terrorism in all its complexities. The global campaign against terrorism cannot be reduced to a slogan slandering Islam or any other religion or race. It is also important to examine the reasons that, despite the global campaign to counter terrorism, the threat continues to evolve and emerge in new and more virulent and toxic forms and ideologies and across ever-extending geographic regions, thereby posing a pervasive threat to international and national peace and security.

Pakistan remains convinced that in order to defeat and eliminate terrorism it is essential to address the underlying causes that create terrorist recruits: unresolved internal and inter-State conflicts, the illegal

use of force, external aggression and intervention, foreign occupation, denial of the right to self-determination, political and economic injustice and the marginalization and alienation of communities and groups. It is only by addressing those underlying causes that the international community can erode the appeal of the narratives of hate and hostility that provide the oxygen for the existence and the growth of terrorism.

The President: I now give the floor to Meszaros.

Mr. Meszaros: The North Atlantic Treaty Organization (NATO) allies and the international community as a whole confront a wide range of terrorist challenges that pose a direct threat to the security of our populations and to international stability and prosperity more broadly. We have faced terrible terrorist attacks on our soils and in our cities. In the changing security environment, NATO is strengthening its capabilities for deterrence and defence. That means investing in and improving military capabilities, but it also means improving nations' resilience to the full range of threats, especially those that are aimed directly at soft targets, such as our civilian populations, our critical infrastructure, our cybernetworks and our essential Government functions. That is why at the Warsaw Summit NATO Heads of State and Government committed to enhancing resilience in those and other critical areas.

More important, from the perspective of critical-infrastructure protection, NATO nations agreed to meet resilience requirements in seven sectors: continuity of Government, energy supplies, civilian supplies, civilian transportation systems, civil-communication services, food and water supplies and the ability to deal with mass casualties and large-scale refugee movements. Those requirements define the level of resilience that allies require in order to be able to counter the full range of threats. NATO member nations are now doing what is necessary to meet those requirements.

For NATO, building resilience is in the spirit of article 3 of the founding Washington Treaty, which obligates every ally to do what is necessary in order to be able to resist attack. But in an age of global interconnectedness, we note that our own resilience is directly linked to the resilience of our neighbours. That is why NATO's work to improve resilience and protect critical infrastructure also includes our partners. If our partners are more resilient, NATO will be more secure.

The Warsaw Summit commitment therefore underlined the need to provide continued support for partners and improve cooperation with other international organizations in order to address vulnerabilities and make the alliance, NATO's neighbourhood and the wider international system more secure. No single entity holds all the tools necessary to achieve resilience.

Accordingly, we are working with the European Union to bolster resilience to hybrid threats and are offering capacity-building assistance to partners in Eastern Europe, South-East Europe, North Africa and the Middle East, particularly in establishing robust crisis-management systems and in training. We are taking this work forward by engaging our partner nations, the private sector and our counterparts in the European Union on the resilience-baseline requirements so as to ensure transparency and compatibility and to foster a sense of shared responsibility.

NATO can act as a platform for allies and partners to share expertise and best practices, but also eventually to provide training and awareness-raising in the area of the protection of critical infrastructure and on wider counter-terrorism issues. We stand ready to share best practices and lessons learned as appropriate with the relevant United Nations bodies, in particular the Counter-Terrorism Implementation Task Force and the Working Group under its auspices. Taking into account our interconnectedness with others, we consider resilience and critical-infrastructure protection to be a shared responsibility, and we stand ready to contribute NATO's experience and expertise to the wider international efforts to enhance resilience.

The President: I thank Mr. Meznaros for his briefing.

I now give the floor to the representative of Kuwait.

Mr. Alotaibi (Kuwait) (*spoke in Arabic*): We would like to thank you, Sir, and congratulate you on assuming the presidency of the Security Council. We would also like to congratulate you on the adoption of resolution 2341 (2017) this morning. Let me also take this opportunity to thank the Swedish presidency of the Security Council during January.

Turning to the topic of today's debate, I would like to thank you for the concept note that your delegation has provided (S/2017/104, annex), as well as all previous speakers for their constructive statements.

Terrorism is a danger that threatens international peace and security and targets innocent civilians — women, children and the elderly — as well as critical civilian infrastructure. In 2015, we suffered a terrorist attack in Kuwait that targeted religious institutions and caused many casualties. In 1990, while our country was occupied by Iraq, oil sites were targeted, thereby undermining our country's environment. That is why we called for the designation of 6 November as the International Day for Preventing the Exploitation of the Environment in War and Armed Conflict.

Kuwait has undertaken many measures to protect its infrastructure. We support the efforts of the international community to combat the Islamic State in Iraq and the Levant. We condemn terrorism in all of its forms and manifestations. Terrorist acts are unjustifiable. They cannot be linked to any religion or nationality. The fight against terrorism requires bolstering international efforts, while also fully complying with human rights, the rule of law, good governance, peaceful coexistence among religions and respect for all religious symbolism. In that respect, we stress the need for the implementation of, inter alia, resolutions 1373 (2001), 1963 (2010), 2129 (2013) and 2322 (2016).

We also stress the need to implement the Global Counter-Terrorism Strategy and support the Counter-Terrorism Committee Executive Directorate along such lines. We emphasize the importance of technical assistance and capacity-building aimed at protecting critical infrastructure while strengthening dialogue between countries and regional and international organizations with a view to exchanging best practices and drawing upon each other's experiences. We also note the importance of international cooperation with INTERPOL, inter alia, in the area of information- and expertise-exchange in order to combat terrorism and improve the protection of critical infrastructure.

We urge all Member States to draw upon the work of United Nations programmes and specialized agencies, as well as regional and international organizations. Critical infrastructure across the world is a particular target for terrorists, as its connectivity makes it more vulnerable to attacks. Information technology entities, when attacked, can become a multiplying factor for danger. That is why there must be cooperation among Governments to devise emergency plans.

Here we would take note of resolution 2286 (2016), on the protection of medical facilities, personnel and equipment in armed conflict. The resolution is fully in line with international humanitarian law and human rights law.

In spite of terrorism continuing unabated and the fact that ISIL is still continuing with its heinous acts, in addition to those committed by Boko Haram, Al-Shabaab and the Al-Nusra Front, in Yemen, Syria, Iraq, Libya, Somalia, these groups continue to lose ground in many regions across the world, as noted in the Secretary-General's report contained in document S/2017/97. We stress the importance of collective action to rebuild critical infrastructure, and we highlight Kuwait's assistance to displaced persons and refugees, as well as the need to rebuild critical infrastructure destroyed by terrorism, so as to ensure that life goes back to normal in hospitals and schools that have been struck as well as other sites.

Finally, we reiterate that our unchanged position of condemning terrorism and stress the importance of international law, the four Geneva Conventions and the relevant Security Council resolutions, as well as international cooperation within the United Nations to tackle this threat.

The President: I now give the floor to the representative of the Bolivarian Republic of Venezuela.

Mr. Ramírez Carreño (Bolivarian Republic of Venezuela) (*spoke in Spanish*): In order to ensure the smooth running of this meeting, I will now read a summarized version of the statement that the Bolivarian Republic of Venezuela has the honour to address to the Council on behalf of the Non-Aligned Movement. The complete text of the statement will be published on the page of the presidency of the Coordinating Bureau of the Movement. After reading out the summarized version, I will then make a few remarks in my national capacity.

First and foremost, I should like, on behalf of the States members of the Non-Aligned Movement, to convey our respects to Mr. Pavlo Klimkin, Minister for Foreign Affairs of Ukraine. We also wish the Ukrainian delegation and Ambassador Volodymyr Yelchenko a very successful month in guiding the work of the Security Council. I wish also to take this opportunity to pay tribute to the very diligent way in which the Swedish delegation, under the leadership of Ambassador Skoog, led the work of the Council during the month of January.

During the seventeenth summit of the Non-Aligned Movement, held in September 2016 on Margarita Island, Venezuela, the Heads of State and Government reaffirmed that terrorism constitutes one of the major threats to international peace and security and reiterated that any act of terrorism is criminal and unjustifiable, irrespective of its motives and of wherever, whenever and by whomsoever committed, as it also constitutes a flagrant violation of international law.

By the same token, the Heads of State and Government reaffirmed that terrorism cannot and should not be associated with any religion, nationality, civilization or ethnic group, nor should such associations be used to justify terrorism or measures to fight it, including, inter alia, profiling or intrusions into individual privacy.

The most recent terrorist attacks, particularly those committed by Da'esh, demonstrate that vulnerability to this scourge and to the phenomenon of foreign terrorist fighters is now global. In this regard, it should be noted that the destruction of the physical and economic infrastructure of States, including critical infrastructure, has always been a major goal of terrorist groups. This sows terror among the general public and also generates massive publicity at the global level.

The protection of critical infrastructure plays a significant role in the fight against terrorism and its prevention and could be incorporated in a comprehensive way into national plans to combat this scourge and prevent it. We therefore need to strengthen international and regional cooperation, in particular through the adoption of timely and effective measures to eliminate this scourge and the establishment of relevant partnerships; this will be very important.

The Movement is of the view that the fight against terrorism must be waged in strict adherence to existing regional and international instruments in this area, including the purposes and principles of the Charter of the United Nations, human rights and fundamental freedoms, in line with the rule of law and obligations under international law.

Moreover, the provision of technical assistance, on request, for capacity-building and the development of appropriate infrastructure, mechanisms and processes, including through the exchange of information, good practices and the identification of areas of vulnerability, will all be decisive in the fight against terrorism.

In this regard, the support and the resources that the United Nations Counter-Terrorism Centre could provide to Member States upon request and in line with its mandate would be very useful in efforts to combat and prevent terrorism. The same is true of the expertise that could be provided to Member States that make such a request by the Counter-Terrorism Implementation Task Force Working Group on Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security.

In conclusion, the Non-Aligned Movement reiterates its full commitment to the fight against terrorism. It is important that we undertake such efforts in a frank, decisive and coordinated manner, including through the full and balanced implementation of the relevant United Nations resolutions and the Global Counter-Terrorism Strategy. Likewise, we must also adopt in the near future a comprehensive convention on international terrorism under the auspices of the United Nations, which would strengthen multilateral cooperation in this area.

I should now like to make a few remarks in my national capacity.

We wish to emphasize the fact that Venezuela's position in response to the threat posed by terrorism in all its forms and manifestations has been reiterated on various occasions in the bodies charged with addressing this issue. We have always robustly condemned terrorist acts, irrespective of their motivations or perpetrators, because of their egregious effects on international peace and security, human rights and development. During our membership in the Security Council, we lobbied hard for the strengthening of international cooperation efforts to prevent, combat and eliminate the horrific phenomenon that is terrorism. We also made it clear that we needed to take a comprehensive approach to the issue of terrorism.

We welcome the adoption today of resolution 2341 (2017) as well as the resolutions adopted by the Council last year, particularly resolution 2286 (2016), on the protection of hospitals and humanitarian personnel in conflict situations.

We are convinced that an effective fight against terrorism requires a shift away from the policy of double standards and other misconceptions that hamper the united efforts of Member States to achieve concrete results for international peace and security. Unfortunately, in recent years terrorism has been

boosted by interventionism and the armed aggression of foreign Powers, of which fraternal countries such as Iraq, Libya and Syria, among others, have been victim. This is aimed at overthrowing legitimately established Governments and has provoked the collapse of the institutional fabric of those States and made them vulnerable to violence and to the narrative of hatred and intolerance promoted by terrorist groups.

Nor can we ignore the terrorist acts perpetrated by State actors, such as the terror sown by the Israeli military aggression almost three years ago against the Palestinian population of the Gaza Strip. That caused the loss of human lives, including women and children, and the destruction of critical infrastructure essential for the alleviation of the already dramatic humanitarian situation of the Palestinians resulting from the imposition of an illegal blockade since 2007. Hospitals, drinking water services, access roads and schools, among other targets, were indiscriminately and deliberately bombed during that armed conflict to punish and attack all the civilian population. The aftermath of the destruction continues to be felt today. It manifests itself in a population beset by despair as they confront a reconstruction process hampered by the policies of the Israeli authorities that block access to materials and services.

For that reason, when we speak of the prevention and fight against terrorist barbarism, it is necessary to bear in mind that policies of interventionism and foreign occupation are a fundamental cause of instability, and therefore constitute favourable conditions that contribute to the birth and expansion of violent non-State actors who become terrorist groups. In that regard, we call for the cessation of armed aggression and interventionism in the internal affairs of countries as illegal practices of foreign policy as elements of power at the international level.

Likewise, any sincere discussion about the scope of the strategy to successfully confront the terrorist threat necessarily involves recognizing the current problem of financing, training and supplying weapons to violent non-State actors by foreign Powers.

Those factors have had a serious impact on the peace, stability and development of Syria, Iraq, Libya and other nations affected by terrorism, with the well-known consequences of the destruction of critical infrastructure, including the productive apparatus and cultural heritage, the use of chemical weapons against the civilian population, and massive violations of human rights and international humanitarian law. Those opprobrious acts constitute a list of war crimes.

The fight against terrorism in general and the protection of critical infrastructure in particular requires that the international community activate a global strategy against terrorism that includes, on the one hand, a genuine cooperation scheme based on international law, and, on the other, an impetus to national public policies to prevent and combat terrorist acts. Those must be designed and implemented in accordance with the rule of law, including respect for human rights and without generating discrimination or prejudiced views of an ethnic or religious nature that could be a breeding ground for resentment and violent extremism promoted by terrorist groups. In that regard, we sympathize with those countries whose citizens may be included in restrictive lists for no other reason than their national origin and religious faith. We believe that this approach is not an appropriate way to deal with the terrorist threat.

Finally, we reiterate that the United Nations and its States Members are responsible for overseeing the effective and timely implementation of General Assembly and Security Council resolutions and of the obligations arising from the relevant international treaties in order to address this global phenomenon and to safeguard critical infrastructure and the population from the indiscriminate violence of terrorist groups.

The President: I now give the floor to the representative of Jordan.

Ms. Bahous (Jordan) (*spoke in Arabic*): I would like to begin my statement today by thanking Ukraine for organizing this open debate and by congratulating it on assuming the presidency of the Security Council for this month. I wish it every success. We also thank the briefers for their statements. In Jordan we too welcome the adoption of resolution 2341 (2017) today, which will undoubtedly represent an important addition to the current state of work in combating terrorism in general and in increasing protection for critical infrastructure in particular.

Terrorism continues to be one of the most important threats to world peace and security. The horrendous attacks around the world by entities such as Da'esh and the growing phenomemon of foreign fighters are proof of the global nature of terrorism, which now targets critical infrastructure as well as individuals. We have

seen the targeting of tourist sites and airports, seaports, oil facilities, energy plants, water facilities, bridges and roads and information systems. These all directly impact other service sectors and lead to a situation of fear and distrust towards State institutions. Therefore we cannot separate the protection of critical infrastructure from the general framework of countering terrorism, and we must protect infrastructure as an integral part of all efforts aimed at improving security and the protection of all potential targets.

That should be done by implementing the United Nations Global Counter-Terrorism Strategy, in addition to including and developing national plans on counter-terrorism to include protection of critical infrastructure. In that context, we must emphasize the importance of strengthening international and regional cooperation in responding to that threat, and of protecting lives and infrastructure more effectively through moving forward in developing the mechanisms that could build capacities in countries so that they can protect their infrastructure, and through sharing information, experience and intelligence between the United Nations and other organizations, such as INTERPOL.

In that regard, we reiterate our support for the Secretary-General in establishing an office for countering terrorism. We hope that it will strengthen United Nations efforts, increase their coherence in countering terrorism and guarantee a balanced implementation of the United Nations Strategy. We reiterate the importance of continuing the Working Group on Infrastructure Protection so that it can continue to support countries to combat terrorism in an international context, by activating public and private sector partnerships and by developing an expert panel on information systems in this connection.

We believe that human resources are the most important factor in countering terrorism and protecting infrastructure from armed attacks or through social networks. In alliance with NATO, Jordan held a workshop on investing in human resources as a most important priority to counter terrorism through spreading values of coexistence and tolerance, particularly in the minds and hearts of youth.

In conclusion, I emphasize Jordan's continued approach to counter-terrorism in seeking to uproot terrorism from its sources. We have always emphasized the importance of increasing cooperation among all parties to confront this scourge, because we are convinced that terrorism can be eliminated only through a common international effort and the sincere political will of all parties.

The President: I now give the floor to the representative of Algeria.

Mr. Bessedik (Algeria) (*spoke in Arabic*): I would first like to congratulate Ukraine on assuming the presidency of the Security Council for this month, and to wish the Ukrainian delegation every success.

My delegation aligns itself with the statement delivered earlier by the representative of Venezuela on behalf of the Movement of Non-Aligned Countries.

(*spoke in English*)

I would like to express my delegation's appreciation for the convening of today's open debate and the relevant choice of topic, one whose connection to the security of my country and the life and well-being of my people is critically important. We would like to take this opportunity to once again reiterate our strong condemnation of terrorism in all its forms and manifestations, regardless of motive and wherever, whenever and by whomever it is committed. Algeria also reiterates its determination to continue fighting terrorism and violent extremism, as well as warning against any misconceptions or tendentious associations of terrorism with specific religions, civilizations or geographic areas.

From our point of view, the fight against violent extremism and terrorism must also include the fight against xenophobia and Islamophobia. Algeria strongly believes that preventing and combating terrorism, including protecting critical infrastructure from terrorist attacks and threats, require a high level of vigilance and mobilization. It is clear that this battle cannot be limited exclusively to the security dimension; it must deploy a coherent national strategy, upstream and downstream.

In the specific area of the protection of infrastructure, Algeria has enacted significant qualitative measures and made major efforts that have helped to ensure a secure environment for all its infrastructure, public and private. We won our battle against terrorism, a scourge that affected much of our national infrastructure during the 1990s. In addition, we have taken significant steps to ensure the security of our borders. The protection of our infrastructure remains at the heart of our national strategy, through action that is well coordinated among

the various security forces, each in its specific field of action.

Resolution 2341 (2017), adopted earlier today, puts the emphasis on international cooperation and timely information-sharing. For its part, Algeria's efforts to combat terrorism and to improve regional and international awareness and cooperation in that connection predate the manifestation of major international acts of terrorism. From the beginning, we have striven to strengthen anti-terrorism efforts at the national, regional and international levels. We would like to underline the importance of consolidating efforts with the United Nations Global Counter-Terrorism Strategy by enhancing cooperation at bilateral, regional and international levels, strengthening capabilities and exchanging best practices and expertise on combating terrorism.

Algeria continues to make every effort to enhance coordination and cooperation, especially in the Sahel region. The current context requires both coordination and strengthening the capacities of the countries of the region on the basis of the principle of ownership. Algeria has engaged in a concerted approach via many cooperation mechanisms, thereby ensuring a great contribution to facilitating the deepening of security cooperation among the countries concerned, by coordinating and strengthening border-control measures and sharing intelligence. The significant military forces deployed at Algeria's borders participate in the Government's efforts to ensure not just our own national security but also that of our neighbours.

While we support the importance of protecting critical infrastructure against terrorist attacks, we firmly believe that the battle against that dreadful scourge must be waged every day and in every area of activity, whether political, institutional, economic, cultural, religious, educational or social. Any hope of success requires the active involvement of all national institutions, all societal stakeholders and all citizens.

Lastly, Algeria will remain actively engaged in efforts to counter terrorism and violent extremism at every level, and will contribute constructively to advancing efforts to put an end to terrorism, including through the work of the General Assembly.

The President: I now give the floor to the representative of the Syrian Arab Republic.

Mr. Mounzer (Syrian Arab Republic) (*spoke in Arabic*): I would first like to thank you, Mr. President, for organizing today's important meeting. I would like to affirm Syria's support for the Security Council's credible and genuine efforts to combat terrorism, which reflects the international unanimity about the fact that today terrorism is one of the world's greatest challenges, and that the international community, through the United Nations and the Security Council, must do its part to coordinate our efforts and cooperation aimed at countering terrorism and extremist ideology. The war against terrorism is a cultural and information battle, not just a military one.

For the sixth consecutive year, my country has been a target for terrorism through the systematic destruction of its technological and educational installations, economic, cultural and social infrastructure and historic sites. This atrocious assault has targeted dozens of hospitals, medical buildings, schools, universities and other centres of culture and education, besides destroying power stations, road networks, bridges, railways and telecommunications and Internet links.

Terrorist armed groups, with the support of known Governments, have continued to commit their terrible acts, some of the worst of which have been the targeting of historical, religious and civilizational sites in Syria, particularly in Palmyra, Aleppo, Maaloula and Idlib, destroying or mutilating many ancient and historic sites and monuments — churches, convents, mosques, temples, mausoleums and theatres, all defaced or destroyed in a barbaric manner. None of this has anything to do with human civilization. From the very beginning, certain Governments have partnered terrorists in Syria by financing and manipulating them, or by imposing coercive, unilateral economic measures against the Syrian people. That has had a devastating effect on various service sectors, on the economy, education and health, and on Syrians' lives. It also reduced the Syrian Government's ability to meet its citizens' needs. To all that must be added the crimes committed by armed terrorist groups against Syria and its people and infrastructure.

The unfortunate irony is that the very Governments that utilize the United Nations as a platform attempt to talk about the humanitarian tragedy experienced by the Syrian people are themselves causing it. In the framework of the very same policy, they target Syrian infrastructure. Illegal military intervention occurs under the guise of what is referred to as the

international coalition, which violates the Charter of the United Nations and international law and targets Syria. These individuals justify their actions — which violate Article 51 of the Charter and the sovereignty of Syria — by professing to fight Da'esh or against terrorism in general,

We have sent many letters to the Secretary-General and to the President of the Security Council that contain accurate information and statistics on the harm inflicted on civilian Syrians and the damage to economic infrastructure, social services, education and oil and gas refineries, damage totalling more than $120 billion. Such damage was caused by the atrocities, the military and air strikes by the so-called international coalition, targeting the Syrian people and their infrastructure.

The Syrian Arab Republic reiterates its appeal to the United Nations and the international community to implement Security Council resolutions seeking to combat terrorism so as to prevent terrorists, sponsored by others, from receiving financial, technological, telecommunications and other support given in the name of personal agendas. Those Governments should compensate the Syrian people and the Syrian Arab Republic itself for destruction of Syrian infrastructure. If not, Security Council resolutions and statements by the representatives of Member States will not go beyond the Council Chamber and the Organization's official records and other documents. That would send the wrong message to terrorists and the sponsors of terrorism.

The President: I now give the floor to the representative of the Netherlands.

Mr. Van Oosterom (Netherlands): I thank you, Mr. President, for organizing today's important open debate on the protection of critical infrastructure against terrorist attacks.

The Netherlands aligns itself with the statement made earlier by the observer of the European Union. We also support the statement made by His Excellency Mr. Vincenzo Amendola, Undersecretary of State of Foreign Affairs and International Cooperation of Italy, in the context of the split term in the Security Council for the period 2017-2018.

I will focus on our national approach to protect our own critical infrastructure, on some lessons derived from it and on the need for international cooperation. My full text will be available via Twitter.

In our national approach, we believe that it is important to have a comprehensive framework to determine the threats that pose a danger to our national security, including to our critical infrastructure. We should have a comprehensive framework to address those threats. The protection of a critical infrastructure is part of the national security strategy in the Netherlands. It is based on the answer to three questions. First, what threatens us and how bad is it? Secondly, what are we already doing to address the threats and what more can and must we do? Thirdly, how do we implement the necessary policies and strengthen our capacities?

The answer to the last question in particular is key, and of course it is complicated. Eighty per cent of the critical processes that make up our vital infrastructure are owned by private actors. Engaging them is not a choice, but a necessity. But many other actors, such as semi-government bodies, play an important role as well. In our approach, those critical providers, as we call them, are themselves first and foremost responsible for the continuity and resilience of the critical infrastructure they own. The national Government provides legal and policy frameworks and oversight and inspection.

There are some lessons that we drew from our own national experiences in our own context. In the Netherlands, we follow a general approach to the protection of our critical infrastructure. This includes the threat of terrorist attacks. By assessing the risks of different types of threats in the same way, the risks become comparable, and that makes it easier to prioritize. With the help of the public and the private sectors, we have compiled a complete list of critical infrastructure, containing two categories of vital processes, A and B. Disruption of A processes has greater consequences than the disruption of B processes. That allows for more effective and efficient allocation of means.

We also work with a counter-terrorism alert system. If our intelligence services detect a serious terrorist threat to a particular vital process, providers and other stakeholders are immediately informed. At that moment, predetermined, heightened security plans are triggered to reduce the threat and limit the potential effects of a terrorist attack.

That brings me to my third point, the need for international cooperation. National efforts are important, but a response to terrorist threats against critical infrastructure can never be only national. Critical infrastructure, such as airports, energy systems

and the Internet, are international by their very nature, and therefore our response to threats in that regard should be equally international.

In that spirit, last week my Government approved our first international cyberstrategy. It outlines where and how to cooperate with international partners to ensure a free and open cyberdomain, safe from terrorists. According to our Minister for Foreign Affairs, Mr. Koenders, by cooperating in coalitions with other countries, we can better counter the threats we face. Security Council resolution 2341 (2017), which the Netherlands co-sponsored, was drafted in the same spirit. I commend Ukraine for facilitating the unanimous adoption of resolution today.

As mentioned in the resolution, the first important step towards an international response is greater sharing of information and know-how. We have to be creative and think outside of the box to get the right people around the table. The Netherlands currently co-chairs the Global Counter Terrorism Forum together with Morocco, and we are very supportive of the initiative launched in that Forum by the United States and Turkey on the protection of soft targets. Its focus is broader than only critical infrastructure, with a set of non-binding good practices that will be produced and be relevant for the United Nations and its Member States in our future work on today's topic.

We must learn from our experiences to prevent terrorist attacks against critical infrastructure as much as possible. We must be well prepared in case an unfortunate incident does occur. And, most important, we must do all of that together. Terrorism knows no boundaries; neither should our cooperation to fight it. We should be better prepared. We should be better protected. We should have stronger partnerships. We should work better together.

The Kingdom of the Netherlands stands ready to continue its cooperation with the United Nations and its States Members in protecting our way of life from terrorists. We will continue to be the Council's partner in making the world a safer place.

The President: I now give the floor to the representative of Brazil.

Mr. Vieira (Brazil): I thank you, Mr. President, for organizing today's open debate. I would like to extend my gratitude to the Chef de Cabinet of the Secretary-General, Ms. Maria Luiza Ribeiro Viotti, and to all other briefers.

Brazil is aware that no country is immune to terrorism and has been attentive to prevention domestically and at the regional and subregional levels. We recently updated our legislation to include the crimes of preparatory acts of terrorism and of recruitment of foreign terrorist combatants. We also simplified the procedures for freezing the assets of terrorists so listed by the Council. We were successful during the 2014 World Cup and in the last year's Olympic Games, when we consolidated inter-agency cooperation, at both national and international levels, to specifically prevent acts of terrorism or the entry of suspected terrorists to critical places like airports.

Critical infrastructure is indeed a preferred target of terrorist organizations. The disruption of the provision of basic services can, after all, have a destabilizing effect in our societies. As highlighted in the concept note (S/2017/104, annex) prepared for this debate, one of the side effects of the advances in information and communication technologies (ICTs) is the increased vulnerability of critical infrastructure. Establishing norms that identify and proscribe the misuse of ICTs and a framework to enhance cooperation among States in countering it would contribute to better addressing this challenge.

The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security had called on the international community to assist in improving the security of critical ICT infrastructure, developing technical skills and advising on appropriate legislation, strategies and regulation in that area. The need to support capacity-building in less developed countries is integral to any strategy to combat the malicious use of ICTs, and will require greater and sustainable investment in infrastructure and services, capacity-building, the promotion of joint research and the development and transfer of technology. Differences in the ability to use and develop ICTs represents a knowledge divide that perpetuates inequalities, such as between developed and developing countries, and that may increase vulnerabilities in an interconnected world.

The use of the Internet and social media by terrorist groups illustrates the evolving nature of the challenge that we are facing. Those platforms are also being used

for inciting hatred, for recruitment and for unleashing attacks on critical infrastructure. As we seek to counter those trends, we must safeguard the freedom of expression and the right to privacy. In that context, we highlight the joint initiative by Brazil and Germany that led to the General Assembly and Human Rights Council resolutions on that issue (resolution 68/167 and resolution 28/16, respectively).

Repressive measures are necessary but not sufficient to eliminating terrorism. Border control, air and maritime security and law enforcement must be coupled with efforts to address structural factors conducive to terrorism — in particular those associated with protracted social, political, economic and cultural exclusion.

We must take action against measures that do not respect diversity and ignore our common humanity, such as those that associate terrorism with specific cultures, religions or ethnic groups. We must be wary of rhetoric that fuels xenophobia and prejudice. Certain responses to the refugee crisis and to recent migration movements are also of concern, as they might increase rather than decrease the risks associated with violent extremism conducive to terrorism.

Let us also not lose sight of the protracted conflicts that may directly or indirectly fuel terrorist agendas. The failure to deal with ongoing crises in the Middle East, including the Israeli-Palestinian conflict, is a case in point.

Terrorist groups seek to provoke Governments into overreacting, so as to exploit their narratives of abuse and oppression. Counterterrorism will be effective only to the extent that it is consistent with the Charter of the United Nations and other norms of international law, including human rights law and humanitarian and refugee law.

We have noted an increase in the number of letters submitted to the Security Council under Article 51 of the Charter, seeking to justify resorting to military action in the context of counter-terrorism, usually ex post facto. At the most recent open debate on working methods (see S/PV.7740), Brazil stressed the need for follow-up to such communications and for an assessment as to whether the obligations laid out in the Charter were being fulfilled.

There can be no justification for terrorism. Brazil reiterates its commitment to a multidimensional response to that threat and remains convinced that cooperation and dialogue within the United Nations will enhance our capacity to achieve the needed results.

The President: I now give the floor to the representative of Afghanistan.

Mr. Salarzai (Afghanistan): Afghanistan thanks Minister of Foreign Affairs Pavlo Klimkin of Ukraine and his delegation for convening today's debate on the protection of critical infrastructure against terrorist attacks. We are pleased to see so many countries participating in today's discussion, which reflects the importance of the topic under consideration.

Infrastructure provides a key component for the normal and effective functioning of society, enabling citizens' access to fundamental services, such as food, water, shelter, adequate health care, transportation facilities and economic opportunities — each of which are critically important for the stability of any environment. An attack that damages a nation's infrastructure in essence does irreparable harm to the very social fabric of society. The protection of physical and social infrastructure should therefore comprise a key component of any strategy for ensuring peaceful and stable societies.

Terrorism and violent extremism constitute dominant factors of instability in the current international landscape, bringing untold suffering and devastation on peoples and communities. As evident in the case of my country, Afghanistan, and many other countries where terrorists operate, extremist forces have gone to great lengths to advance their vicious agenda — wreaking havoc, undermining the rule of law and terrorizing populations. They openly target many kinds of infrastructure to amplify the effects of their barbarity and to attract global media attention.

Afghanistan has been a primary victim of global terrorism for over two decades — long before the start of the international community's engagement in our country in 2001. Today, our people remain defiant in the face of a multitude of terrorist groups, such as the Taliban, the Haqqani Network, Al-Qaida, Da'esh, Jamaat Dawah, Lashkar i Jhangvi , the Islamic Movement of Uzbekistan and other foreign terrorist fighters, all of which are symbiotically linked to one another, come from abroad and receive, inter alia, political, ideological, moral and material support. Aside from targeting our security forces and those of international partner countries present in Afghanistan, extremists are

attacking our political and legal institutions; mosques and schools; health and medical facilities; and other soft targets, such as non-governmental organizations, which are working to improve the lives of ordinary Afghans.

Just last week, in the continuation of their carnage, a suicide bomber conducted an attack on our Supreme Court, the highest judicial institution in our country, killing 21 people and wounding close to 50 others. The victims included several female judges, prosecutors and court employees who were simply returning home to their families after a hard day's work.

Last month, on 11 January, the Taliban carried out an attack on our Parliament, resulting in more than 120 people dead, with many more left severely maimed or injured. That act of barbarism was widely viewed as an attack on the infrastructure of our democracy, which is among the most significant achievements of Afghanistan since 2001.

In August of last year, extremists attacked the American University in Kabul, which is seen as a beacon of hope for a better future among our educated and talented youth. Sixteen people were tragically killed in that attack.

Moreover, there are many cases of local hospitals, clinics and international humanitarian relief agencies coming under attack or otherwise being negatively affected by the activities of extremist groups. A few days ago, Da'esh militants in northern Jowzjan province killed six members of the personnel of the International Committee of the Red Cross (ICRC) in northern Afghanistan. The ICRC convoy was attacked while travelling to distribute aid to a storm-stricken area.

The overall security environment has only complicated humanitarian conditions for our people, to the point where 9.3 million people, mainly women and children, are in dire need of immediate humanitarian assistance. This figure marks a notable increase from last year. We reiterate our call on the international community to support the 2017 humanitarian response plan of the Office for the Coordination of Humanitarian Affairs.

Terrorists also pose a threat to economic and development infrastructure projects, in which we have invested heavily. We are currently working to implement 18 cooperation and investment projects in the areas of energy, transport and trade and the commercial and labour sectors. Once completed, those projects will benefit the prosperity of Afghanistan and our wider region.

The ongoing cycle of violence in Afghanistan is not, by any means, a homegrown phenomenon. Its roots lie elsewhere, outside Afghanistan, emanating from a strategic plan crafted from within our region to advance an ill-fated political agenda that serves no one, defies international law and constitutes a blatant violation of the very spirit and tenets of the Charter of the United Nations, as well as the relevant counter-terrorism resolutions of the General Assembly and Security Council. We believe the fight against international terrorism stands at a crossroads. At this critical juncture, a refined global effort is needed to combat this menace with greater precision and accuracy. In that context, we welcome the efforts of the Secretary-General to strengthen the United Nations counter-terrorism architecture, including his decision to establsih an office for counter-terrorism and to appoint an Under-Secretary General to head that office.

Despite the difficult security environment in Afghanistan, we are a nation that is making steady progress towards lasting stability and self-reliance. The National Unity Government is working, in greater cohesion and coordination, on tackling a difficult set of challenges facing our people. In that effort, our security forces are serving valiantly to enhance security, while defending and protecting our sovereignty, infrastructure and people against terrorism and violent extremism.

In conclusion, we believe today's meeting marks an important step forward in devising a more effective United Nations approach to protecting critical infrastructure from terrorist attacks. As the principal organ of the United Nations responsible for the maintenance of peace and security, we hope the Security Council will continue to give due focus and attention to this important matter.

The President: I now give the floor to the Permanent Representative of Morocco.

Mr. Hilale (Morocco) (*spoke in French*): Allow me, first of all, to congratulate Ukraine on assuming the presidency of the Security Council for the month of February and for scheduling this open debate on the protection of critical infrastructure against terrorist attacks. The relevance and timing of the issue are testimony to its importance.

Although since the beginning of its existence humankind has sought to create, innovate and build for its own well-being and that of future generations, terrorist groups — on the contrary — have chosen the path of destruction, anarchy, and nothingness. The terrorist threat has continued to grow and spread. Terrorist groups such as Da'esh, Al-Qaieda, the Taliban, Boko Haram and others, as well as their affiliates, are constantly developing new methods of destruction. They miss no opportunity to perpetrate attacks against sensitive and easily accessible elements of infrastructure, including airports, metro stations, trains, buses, hospitals, banks, markets, schools, universities and institutes. The attacks perpetrated against the airports in Brussels and Istanbul, as well as against the train stations of London and Madrid, access to bank data, State establishments are all acts that illustrate the readiness of terrorist groups to attack any part of infrastructure, and to exploit the slightest vulnerabilities in security and monitoring. Even places of worship — mosques, synagogues and churches — have not escaped their macabre acts, despite the fact that they are places the faithful go to in search of peace, tranquility and spirituality. Moreover, nuclear and chemical facilities, storehouses for radioactive material, electricity systems and dams are very sensitive sites and are vulnerable to terrorist acts in the absence of adequate security. They could be turned into weapons of mass destruction.

The terrorist threat has been exacerbated by the phenomenon of the return of foreign terrorist fighters to their countries of origin or third countries. In the most recent report (S/2016/92) of the Secretary-General on the threat posed by the Islamic State in Iraq and the Levant (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat, elaborated in accordance with the resolution 2253 (2015), the Secretary-General warns of the phenomenon of the return of foreign terrorist fighters following the military defeats of Da'esh in several theatres of war. The report estimates the number of foreign terrorist fighters in Iraq and in Syria to be 40,000 individuals from more than 100 countries. As such, the return of those foreign terrorist fighters, well trained in guerrilla tactics and the manufacture of explosives, constitutes a threat to society and sensitive infrastructure. They can act individually as lone wolves, which led the Secretary-General to point out that terrorist organizations have a great capacity for adaptation. He indicated that the threat to civil aviation also remains quite high. That is why the responsibility for protecting sensitive infrastruce lies primarily with States, which must integrate such protection in their national strategies, as well as their strategies to combat terrorism and violent extremism. The State must ensure the implementation of effective means of protection and security, including through the adoption of the necessary legislation in accordance with international standards and requirements.

Morocco has adopted a comprehensive, coherent approach oriented to prevention and action. We believe that terrorism is a global phenomenon that requires and calls for a global response paired with and supported by robust cooperation at the regional, subregional and international levels. Morocco attaches particular attention to international cooperation, strengthened border security, information exchange and sharing, the use of the INTERPOL database and the roll out of deradicalization and re-integration to ensure that terrorist plans fail.

At the regional and subregional levels Morocco engages in the exchange of information, expertise and experience both in the framework of South-South cooperation as well as with African countries, with countries in the Mediterranean basin, including in the framework of the 5+5, and other regional partners. Morocco hosted conferences in 2013 and 2015 on border security in the Maghreb and the Sahel and participated in the 2015 Madrid meeting. Morocco also took part in the Nuclear Security Summit held in Washington, D.C, the final communiqué of which called for greater efforts to prevent non-State actors from obtaining nuclear or radioactive materials for malicious purposes or attacks against sensitive infrastructure.

Finally, conscious of the importance of combating nuclear terrorism, Morocco has actively participated in the Global Initiative to Combat Nuclear Terrorism since its launch in 2006. Morocco participated in all relevant meetings and conferences and even organized several meetings and awareness-raising workshops for its African peers. The experience of Morocco in that area was shared just last week in New Delhi during a meeting of the working group to assess the strategy.

The President: I now give the floor to the Permanent Representative of Poland.

Mr. Winid (Poland): I thank the President for organizing this meeting and introducing the issue of

protecting the critical infrastructure against terrorist attacks on the Security Council agenda.

We align ourselves with the statement delivered by the observer of the European Union earlier today, but I would like to add some comments in my national capacity. While Poland participated in the Arria Formula meeting on this topic, organized by the Ukrainian delegation in November 2016, today we take yet another opportunity to discuss this topic of utmost importance.

Terrorism poses a growing threat to both national and international security. It also violates and abuses human rights, including every basic right to life, and undermines development. The Security Council has repeatedly underlined that terrorism constitutes a threat to the maintenance of international peace and security.

Threats do not respect borders in today's globalized world. Terrorists can easily infiltrate our most vulnerable energy and transportation hubs. It is recommended that we broaden cooperation within a wider geographical context. The United Nations is a proper, or even the best, forum to initiate the discussion of how to do it.

The protection of critical infrastructure is, first and foremost, the responsibility of national authorities. The ultimate condition for achieving that protection is to have efficient national security systems. However, there is also space for closer international cooperation. That results from the fact that the potential threats are of a transboundary nature and that many useful lessons learned can be shared among States. In that context, Poland is ready to share its experiences with partner countries and to support security-sector reform programmes.

One good example of such cooperation, which Poland and Ukraine have initiated, concerns chemical security, including critical chemical infrastructure. Projects dedicated to that area have also been developed, both bilaterally and multilaterally, in the Organization for Security and Cooperation in Europe (OSCE) and the European Union (EU) and have been supported by the Group of Seven's Global Partnership: Chemical Security Sub-Working Group. The continuation of those efforts is becoming more and more important, owing to the fact that many chemical facilities are located in Ukraine, in particular in Donetsk and Luhansk, the areas affected by the hostilities and the war imposed on Ukraine from the outside.

Poland and Ukraine also shared close cooperation in 2012 when we co-hosted the Union of European Football Associations European Championship. That collaboration included, among other things, the protection of transportation infrastructure and the provision of the safety and security needed for organizing mass sporting events.

Let me also highlight the growing role of the international aspects of critical-infrastructure protection. Regional organizations, such as the OSCE and the European Union, have introduced programmes aimed at structured cooperation and the exchange of information. For instance, the OSCE framework includes travellers' security and the protection of energy infrastructure. The EU cooperation envisages an air-passengers database, cooperation among border guards and European Police Office reports. It has been recommended that cooperation in this area be extended into a wider geographical context. The role of the State-private sector link is also quite vital.

Finally, let me welcome resolution 2341 (2017) on the protection of the critical infrastructure, which was initiated by Ukraine and adopted this morning with the co-sponsorship of Poland.

I thank you once again, Sir, for organizing this meeting.

The President: I now give the floor to the representative of Canada.

Mr. Bonser (Canada): Canada is proud to have co-sponsored resolution 2341 (2017) today.

Terrorist groups are evolving, and we need to continue to work to understand their strategies in order to protect our populations. For example, as Da'esh faces losses in Iraq and Syria, it is transforming from a territory-based entity into a global virtual network. Foreign terrorist fighters still loyal to D'aesh and with training and battlefield experience pose a renewed threat as they move to new locations. The threat of lone actors inspired by violent extremist ideologies persists. As terrorists seek to impose maximum damage in new areas of operation, critical infrastructure is a vulnerable target.

Attacks on physical assets, information-technology systems, networks and services essential to health, safety and security can be devastating in terms of loss of life and the harm they can cause to the collective economic well-being and the erosion of the public's

sense of safety. Attacks that succeed in inflicting great harm and damage also bolster the propaganda efforts of terrorist groups. Member States must work together in a coordinated effort to respond to that aspect of the global terrorist threat as an integrated part of our collective efforts. We therefore welcome today's resolution, presented by Ukraine, which encourages Member States to develop or further improve their strategies for reducing risks to critical infrastructure from terrorist attacks.

In our national context, Canada is working to leverage our critical infrastructure networks to share information and strengthen our resilience against terrorist attacks. Canada's national strategy and action plan for critical infrastructure establishes a collaborative federal, provincial and territorial approach to the security of the critical infrastructure sector so as to mitigate the full range of risks and threats facing Canada's vital assets and systems. The national strategy aims to build partnerships, implement an all-hazards risk-management approach and to advance the timely sharing and protection of information among partners. Ultimately, protecting our vital assets and systems from threats demands a cooperative approach across a broad range of stakeholders at every level.

(*spoke in French*)

We underscore the need for legal and regulatory frameworks to address this threat and encourage United Nations agencies to incorporate that into their needs assessments aimed at supporting Member States' capacity-building efforts. We appreciate the resolution's language reinforcing the protection of critical infrastructure as part of a holistic national/global counter-terrorism strategy that balances vital security concerns with rights and freedoms. Canada wholeheartedly endorses cooperation in that area within and among Member States at all levels. We firmly support the resolution.

In conclusion, we take this opportunity to underscore Canada's strengthened commitment to inclusion and diversity, following the massacre targeting a mosque in Quebec City that killed six Canadians this past January. As Prime Minister Justin Trudeau said at the 2 February funeral service for three of the victims,

> "We will combat all extremism in any form and ... we will be there for all citizens and protect their fundamental freedoms — the freedoms of religion and of conscience — so that anyone can fulfil their destiny"

in complete security.

The President: I now give the floor to the representative of Malaysia.

Mr. Onn (Malaysia): I wish to thank you, Sir, for convening today's open debate, and I join earlier speakers in congratulating you on your delegation's assumption of the presidency of the Security Council for this month. I also wish to thank the briefers for their briefings and insights on today's issue.

Malaysia stands firm in the fight against terrorism. It is without a doubt that damage to the critical infrastructure that is essential for the maintenance of vital societal functions, whether through natural disasters, terrorism, criminal activity or malicious behaviour, has a negative impact on the security of a country and the well-being of its citizens. It is therefore important that national critical infrastructure be protected against terrorist attacks.

All Governments recognize the threat posed by terrorism against critical infrastructure and the sustained preventive and mitigation efforts that such threats demand. While the responsibility for the protection of critical infrastructure against terrorist attacks rests primarily with the State, the implementation of steps to reduce the vulnerability of privately owned and corporate assets is also highly dependent on the owners of such assets.

Nevertheless, private firms may not have adequate commercial incentives to fund initiatives to reduce vulnerability. For some, the cost of reducing vulnerabilities may seem to outweigh the benefits of reduced risks from terrorist attacks, as well as from natural and other disasters.

While Governments have a primary role to play in the protection of critical infrastructure, it is a matter of responsibility, necessity and good governance for the owners of such critical infrastructure to address the security needs of their assets. There is therefore a need for Governments and businesses to share intelligence and information on threats and vulnerability and on measures to protect infrastructure and mitigate the risk involved.

We believe that the Counter-Terrorism Implementation Task Force's Working Group on

the Protection of Critical Infrastructure Including Vulnerable Targets, Internet and Tourism Security has an important role to play in the international community's efforts to protect critical infrastructure against terrorist attacks. Those efforts may include promoting international and public-private cooperation; capacity-building; the sharing of best practices; improving responsiveness and resilience through planning, prevention, crisis management and recovery; promoting the exchange of information and best practices; and establishing a network of experts on the protection of critical infrastructure.

At the domestic level, Malaysia's efforts in the area of the protection of critical infrastructure are divided into two levels, namely, the federal level and the state level. At the federal level, those efforts fall under the Central Committee on Critical National Infrastructure, which is led by the Secretary General of the Ministry of Home Affairs. At the state level, the Committee on Critical Infrastructure is led by the State Secretary. Under these committees, the audit or monitoring teams have been tasked with monitoring the level of security at all critical infrastructure sites in order to detect any non-compliance and to advise the operator or owner accordingly on how to improve the security level in the entities concerned. National legislation related to the protection of critical infrastructure against terrorist attacks includes the National Security Council Act 2016 and the Protected Areas and Protected Places Act 1959. A national cybersecurity policy is also in place aimed at ensuring the security of Malaysia's critical national information infrastructure.

Malaysia's sponsorship of resolution 2341 (2017), adopted by the Council earlier this morning, signifies Malaysia's commitment to the efforts of the international community in this field through the sharing of best practices, experience, expertise and intelligence aimed at further strengthening our capacities to safeguard and protect critical infrastructure against terrorist attacks.

The President: I now give the floor to the representative of Australia.

Ms. Wilson (Australia): Safeguarding our critical infrastructure is an economic and security imperative. Australia supports Ukraine's initiative aimed at mobilizing international cooperation in the area of preventing and responding to terrorist attacks against critical infrastructure.

The threats posed by terrorism to critical infrastructure are enduring and require sustained mitigation efforts by Governments. The United Nations has a key role to play in that regard, including by working with Member States to ensure the full implementation of the United Nations Global Counter-Terrorism Strategy and the relevant Security Council resolutions.

Countries define what constitutes critical infrastructure in different ways. For Australia, critical infrastructure refers to the physical facilities, supply chains, information technologies and communication networks that — if destroyed, degraded or rendered unavailable for an extended period — would significantly impact the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security.

In January 2017, Australia established the Critical Infrastructure Centre, which provides a coordinated and cohesive approach to the security of Australia's critical infrastructure. The Centre brings together expertise and capability from across the Australian Government to better manage the national security risks to our critical infrastructure. Australia relies upon a strong intelligence-led prevention and preparedness regime to support our counter-terrorism arrangements. That approach encompasses targeted prevention and preparedness measures based on risk-management principles and on maintaining capabilities to manage various types of terrorist threats, attacks and their consequences. The Australian Government also works with owners and operators in a business-Government partnership to share information, tap into the experiences of others and develop collaborative mitigation measures for dealing with the most serious risks to critical infrastructure.

From an information-technology perspective, the Australian Cyber Security Centre is the Australian Government's primary source of advice on cyberthreats. It is firmly of the view that establishing a strong cybersecurity posture, increasing awareness of potential vulnerabilities and implementing effective security measures are vital to efforts to deter and prevent incidents against critical infrastructure, including from terrorists. The safety and security of critical infrastructure require the concerted efforts of public and private partners around the globe. Australia looks forward to continued practical collaboration with international partners, including the United Nations, to

enhance and promote cross-border and global critical infrastructure security and resilience.

The President: I now give the floor to the representative of Latvia.

Mr. Mažeiks (Latvia): Latvia welcomes the initiative of Ukraine, during its presidency of the Security Council for this month, to hold this important debate, which brings the issue of the protection of critical infrastructure from terrorist attacks to the forefront of the international discourse. I thank all the speakers for their valuable briefings.

Latvia aligns itself with the statement delivered by the observer of the European Union (EU).

The spread and intensity of global terrorism is, without a doubt, one of the greatest threats to international peace and security that we face today. In the past year, in Europe alone, we have witnessed a number of heinous acts of terror, some of which were committed ruthlessly and purposefully against critical infrastructure. The attacks on the airport and subway station in Brussels last March illustrate all too painfully that terrorists have spread and will continue to spread fear and disarray by striking where they deem that their attacks will have the most impact.

Attacks on transportation systems, as well as on telecommunications networks, energy infrastructure and water-supply systems, can often multiply the perceived terrorist threat, causing a ripple effect of fear that reaches far beyond those immediately affected by the attack. Therefore, the prevention of such attacks by creating adequate protection measures for critical infrastructure is of paramount importance.

In support of the President's call for the consolidation of international efforts to increase resilience against terrorist threats, Latvia joined the sponsors of today's resolution 2341 (2017) on the protection of critical infrastructure from terrorist attacks.

In Latvia, the measures adopted for the protection of critical infrastructure reflect the common approach established by the European Union and employ the EU tools designed for that very purpose. Our legislation is closely attuned to the requirements set out by the EU directive on European critical infrastructure, thereby contributing to the unification of identification and protection standards for critical infrastructure objects on a regional, European scale.

We have established a cross-sectoral Government commission tasked with the regular identification and assessment of existing and potential critical infrastructure objects in order to improve the safety and security of all potentially critical infrastructure objects. The security and protection requirements for those objects are equally high for nationally, municipally or privately owned structures. Moreover, all structures deemed to be national or European critical infrastructure objects in Latvia have a designated point of contact so as to facilitate the exchange of information with national security institutions. In order to strengthen public-private partnerships and build capacity with regard to the security and protection of critical infrastructure objects, the responsible internal security institutions hold regular training seminars and on-site workshops for both private and public entities tasked with ensuring oversight and the security of critical infrastructure objects.

In the increasingly globalized and interconnected world, the digitalization and integration of critical infrastructure with the help of information and communication technologies add a new sense of urgency for the need for comprehensive and internationally coordinated protection efforts. In our view, that is the area where the United Nations can play a key role by providing the best platform for the exchange of knowledge, experiences and best practices among the Member States.

The President: I now give the floor to the representative of Maldives.

Mr. Sareer (Maldives): Let me begin by welcoming Ukraine on its assumption of the presidency of the Security Council for this month and expressing our appreciation for its organization of today's open debate on the protection of critical infrastructure against terrorist attacks.

Given the insightful briefings provided by those who have spoken before the Security Council today, and in the interests of time, I shall limit our intervention to four key points, relating in particular to the need to take an integrated and coordinated approach in the protection of infrastructure against terrorist attacks.

First, it is essential that efforts to improve the security of critical infrastructure with respect to the threat of terrorism be part of a broader, institutionalized whole of preventing violent extremism and the counter-terrorism agenda at the national level. That is only inevitable,

given the complex and interlinked nature of today's terrorist threats and modern infrastructure networks alike. Work carried out on the basis of strengthening such protection will almost always rely on the strength of counter-terrorism efforts in other areas, coinciding with the aims of other initiatives seeking to prevent acts of terrorism. Duplication needlessly undermines our national efforts and wastes what are usually limited financial, physical and human resources.

Secondly, the need for coordinated efforts is especially strong for small countries, including small island developing States (SIDS) such as the Maldives. Cognizant of those facts, the Government of the Maldives has developed a robust institutional framework for taking a coordinated and whole-of-society approach to countering terrorism and violent extremism through concrete measures and cross-cutting policies. Last year, we implemented a State policy on terrorism and violent extremism and are currently in the process of formulating a national counter-terrorism strategy and counter-terrorism response plan as part of that policy. The implementation of those programmes will be guided by the National Counter-Terrorism Centre, which was also established last year, with an express mandate to lead and coordinate the work of all State institutions with respect to terrorism and violent extremism.

A key component of that State policy is the development of programmes aimed at safeguarding tourist resorts and the travel industry, which is a critical sector of our economy, and security programmes for sea ports, airports and sectors of major economic infrastructure. Those are focal points of policies for protecting critical infrastructure in any country, but their importance is only magnified for SIDS given their small size, geographic isolation and limited resources. A terrorist attack on critical infrastructure would be devastating regardless of where it took place. But whereas an attack, while tragic, would ultimately be local in its impact for a large country in which such infrastructure exists in abundance, for a small island country that relies entirely on one or just a handful of such infrastructural facilities, such an attack would be systemic in its impact. For SIDS, an attack on a sole international airport, sea port, major power plant or water distribution network would not merely exact a costly human toll but cut off an entire people from their livelihoods, material necessities or even the rest of the world.

Thirdly, in the light of the amplified magnitude of the threat for countries, such as SIDS, that face considerable geographic, economic or social constraints, capacity-building and the exchange of best practices are critical if all nations are to be able to effectively respond to such threats. The Maldives is fortunate to have benefited from cooperation with international partners with regard to capacity-building in the security, health-care and public utility sectors in areas that serve to improve its ability to address and respond to those emerging threats to critical infrastructure.

Fourthly, the transnational and increasingly multisectoral nature of contemporary terrorist organizations, particularly with respect to transnational organized crime, requires us to increase, at the bilateral, subregional, regional and global levels, cooperation in countering terrorism and protecting critical infrastructure. Likewise, it means that we must improve the ability of intergovernmental organizations — first and foremost among them the United Nations — to assist in the coordination of counter-terrorism strategies.

In that respect, we must collectively rededicate ourselves to finalizing the comprehensive convention on international terrorism so that we may, at long last, be able to address those issues in the framework of a detailed and comprehensive international legal instrument. We need to deepen both our respective national participation in regional initiatives aimed at countering terror and preventing violent extremism, and our support for multilateral efforts on the part of the United Nations and other intergovernmental organizations, such as the Secretary-General's Plan of Action to Prevent Violent Extremism. In that regard, we take note of the efforts of the Working Group on Protection of Critical Infrastructure Including Internet, Vulnerable Targets and Tourism Security

Just as the threats posed by terrorism to all parts of our societies, including critical infrastructure, continue to evolve, so too must the methods with which we are to respond to those threats. That is and must continue to be a collective, collaborative and coordinated effort for the dangers that we will face. In that aim, Sir, we assure you that you can rely on the Maldives' wholehearted support.

The President (*spoke in French*): I now give the floor to the representative of Haiti.

Mr. Régis (Haiti) (*spoke in French*): I thank you, Sir, for your invitation in French to take the floor.

First, on behalf of the Government of the Republic of Haiti, I would like to thank the Government of Ukraine for its kind invitation to this open debate in the Security Council devoted to a topic of major importance — the protection of critical infrastructure. I welcome the presence of His Excellency the Minister for Foreign Affairs of Ukraine, Mr. Pavlo Klimkin, this morning, and commend him on the quality of his statement and his suggestions on the paths for us to take in reflecting upon the issue and taking action.

The United Nations has made the implementation of the Global Counter-Terrorism Strategy a key priority. The protection of critical infrastructure undeniably plays a major role in that regard. My delegation fully supports the goals of the comprehensive and integrated response Strategy at the national, regional and international levels.

The likelihood of large-scale terrorist acts being committed and targeting civilians through attacks on critical infrastructure has only increased over the past several years. To varying degrees, of course, that danger is felt everywhere. The emergence of new threats, amplified by the rapidly evolving nature of communications technologies, has dramatically increased the probability of such an attack as well as the seriousness of such a threat's consequences with regard to international peace and security.

In the merciless struggle that must be waged against terrorism, Haiti is party to the United Nations counter-terrorism system and to several regional cooperation mechanisms established at the level of the Caribbean Community and the Organization of American States, in particular the Inter-American Committee against Terrorism. At the national level, the Government of Haiti strives to maintain a level of vigilance commensurate with the threats posed by movements influenced by extremist ideologies. To this end, it fully supports international efforts to strengthen the capacity of States to act collectively in the prevention of incitement to terrorism and to improve the security and protection of particularly vulnerable targets, such as infrastructure and public places, as specifically called for by the Global Counter-Terrorism Strategy.

However, we must recognize that, while acts of incitement to terrorism are frequent, the international counter-terrorism regime, particularly with regard to the protection of essential infrastructure, remains tragically inadequate. This is evidenced by the threats, thwarted attacks and incidents by which many countries in Europe, Asia, Africa and America have been targeted in the recent past. If the rise of terrorism seems on occasion to have been slowed, its momentum is far from broken. Its sphere of action, while contained in certain theatres of operation, is elsewhere in full expansion.

It is therefore essential to redouble efforts, intensify international cooperation on all fronts, including judicial and police cooperation, the exchange of information, the provision of relevant and adequate technical assistance to States that require it, in particular the least developed among them, so as to maintain a high level of protection of critical infrastructure, increase resilience against terrorist threats, and prevent the loss of human life and the disruption of essential services, as outlined in the concept note issued by the Ministry for Foreign Affairs of Ukraine (S/2017/104, annex). In that regard, I should like to make a few brief comments on the terrorist threat and the overall response strategy.

First, it is essential to pinpoint the terrorist threat in order to defeat its actions, which no rationale — including the national, political and religious demands generally advanced by the perpetrators — can justify. Terrorism cannot be associated with any religion, nationality or civilization. However, there is undeniably a number of conditions conducive to its spread, be it the perpetuation of regional conflicts that are often at the root of violent extremism, discrimination, exclusion, socioeconomic marginalization, poor governance and poverty.

It is therefore urgent for the international community to address these issues and to provide the developing countries, particularly the poorest among them, with the adequate support they need to acquire the necessary infrastructure and overcome the serious economic and social challenges they face. My delegation, moreover, believes that no State, however powerful it may be and whatever the degree of priority it attaches to the fight against terrorism, can alone achieve the overriding objective of protecting its citizens and its critical infrastructure. Partnerships are therefore essential at the international, regional and national levels. Similarly, regional counter-terrorism mechanisms should be significantly strengthened and adequately resourced in order to enable them to respond more effectively, taking into account the realities and needs on the ground, as well as the evolution of the terrorist threat to critical infrastructure.

Finally, the development of integrated national responses for the prevention of terrorism and the protection of critical infrastructure is of particular importance. In that regard, I offer my delegation's support for the Ukrainian proposal to incorporate a critical infrastructure protection component into all national and international programmes for the prevention of terrorism.

The Government of Haiti, for its part, will continue to pay the utmost attention to measures to prevent and combat terrorism, including those relating to the protection of essential infrastructure. Recent changes have been made to the Haitian penal code, reinforcing the range of legislative and legal measures to prevent and contain ideologies of hatred and violent extremism. The strengthening of the rule of law, the judicial system and law enforcement agencies is one of the main lines of action of the programme of action defined by the President of the Republic, His Excellency Mr. Jovenel Moïse. At his inauguration on 7 February, he reiterated the high importance he personally attaches to the consolidation of the rule of law in Haiti. There can be no doubt that the new Government of Haiti, which shall soon assume power, will stay true to that spirit and strive to take the necessary measures in response to the evolution of the terrorist threat to critical infrastructure.

The meeting rose at 3.45 p.m.