United Nations S/PV.9779

Security Council

Seventy-ninth year

Provisional

9779th meeting
Friday, 8 November 2024, 10 a.m.
New York

President:	Mr. Kariuki	(United Kingdom of Great Britain and Northern Ireland)
Members:	Algeria	Mr. Koudri
	China	Mr. Geng Shuang
	Ecuador	Mr. Montalvo Sosa
	France	Mr. Dharmadhikari
	Guyana	Ms. Persaud
	Japan	Mr. Mikanagi
	Malta	Mr. Camilleri
	Mozambique	Mr. Afonso
	Republic of Korea	Mr. Hwang
	Russian Federation	Mr. Nebenzia
	Sierra Leone	Mr. Kanu
	Slovenia	Mrs. Blokar Drobič
	Switzerland	Mr. Hauri
	United States of America	Ms. Neuberger

Agenda

Threats to international peace and security

The meeting was called to order at 10.05 a.m.

Adoption of the agenda

The agenda was adopted.

Threats to international peace and security

The President: In accordance with rule 39 of the Council's provisional rules of procedure, I invite the following briefers to participate in this meeting: Dr. Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization; and Mr. Eduardo Conrado, President of Ascension.

In accordance with rule 39 of the Council's provisional rules of procedure, I also invite His Excellency Mr. Stavros Lambrinidis, Head of the Delegation of the European Union to the United Nations, to participate in this meeting.

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

I give the floor to Dr. Ghebreyesus.

Dr. Ghebreyesus: I thank France, Japan, Malta, the Republic of Korea, Slovenia, the United Kingdom and the United States for convening today's discussion and for the opportunity to brief the Council on this increasingly important and disturbing topic.

In March 2020, Brno University Hospital in Czechia suffered a ransomware attack that forced it to shut down its network, transfer patients to neighbouring institutions, postpone planned procedures and revert to paper-based processes. That attack occurred just as the nation entered a state of emergency due to the pandemic. In May 2021, the Conti ransomware gang compromised the Irish Health Service Executive. The attack began with a phishing email containing a spreadsheet attachment, which, when opened, downloaded malware. The malware spread throughout the Health Service Executive's network over two months, encrypting about 80 per cent of the data, making the national diagnostic imaging platform inaccessible and pausing radiotherapy services in five major centres. As a result, more than half of acute hospitals postponed outpatient appointments and elective clinical investigations and interventions, with clinical staff resorting to paper-based processes to maintain baseline services.

Let us be clear at the outset that ransomware and other cyberattacks on hospitals and other health facilities are not just issues of security and confidentiality; they can be issues of life and death. At best, such attacks cause disruption and financial loss. At worst, they undermine trust in the health systems on which people depend, and even cause patient harm and death.

The digital transformation of health systems, the high value of health data, increasing demands on health systems and resource constraints all contribute to making health facilities attractive targets for ransomware attacks. Those attacks target the digital infrastructure of health facilities, disrupt or shut them down. In order for access to be returned, the perpetrators demand a fee, or ransom, be paid.

Cybercrime groups operate on the logic that the greater the threat to patient safety, confidentiality and service disruptions they can create, the greater the ransom they can demand. If health facilities do not pay, the consequences are not simply financial and operational; they are potentially putting patients at risk. To restore the system and retrieve the data quickly, health facilities are often willing to pay a substantial ransom, even if there is no guarantee that data will be decrypted or that attackers will not try again.

Surveys have shown that attacks on the healthcare sector have increased in both scale and frequency. That is because of the success that hackers achieved in attacking hospitals and health facilities. In a global survey in 2021, more than a third of respondents reported at least one ransomware attack during the preceding year, and one third of those reported paying a ransom. However, even when ransoms were paid, 31 per cent of respondents did not regain access to their encrypted data.

Although the main focus of ransomware attacks has been on hospitals and other health service providers, the broader biomedical supply chain was also targeted during the pandemic. Security researchers identified vulnerabilities in at least 17 biomedical companies involved in manufacturing coronavirus disease vaccines and developing therapeutics. Further attacks were reported against clinical trial software vendors, laboratories and pharmaceutical companies.

The report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 (see A/79/214) makes many recommendations on measures that Member States can take to strengthen cybersecurity through rules, norms and principles of responsible

State behaviour, international law, confidence-building measures, capacity-building and institutional dialogue. The World Health Organization (WHO) and our partners are working on many of those recommendations as they apply to health.

In December last year, WHO convened experts in Geneva to develop strategies and approaches to addressing cybersecurity threats, especially in resource-constrained settings. They identified several key challenges, including, inter alia, a failure to communicate the threat of ransomware and the value of investing in cybersecurity clearly to decision-makers; the lack of a clear governance framework for cybersecurity; complex infrastructure that is challenging to make more secure; and a significant gap between the global demand and supply of cybersecurity skills and experts.

To close those gaps, WHO and other United Nations agencies are actively supporting Member States with technical assistance, norms, standards and guidance to enhance the resilience of health infrastructure against cybercrime, including ransomware. In January, WHO published two reports in collaboration with INTERPOL, the United Nations Office on Drugs and Crime and other partners on ways to strengthen cybersecurity and counter disinformation. WHO is also developing guidance on implementing and investing in the cybersecurity and privacy protection of digital health interventions, which is be published next year.

Cybersecurity is a whole-of-government responsibility, but health sector authorities, funders and product owners remain accountable for the security of information systems used for health. There are many measures that Member States can take to enhance their cybermaturity, or their level of readiness for cyberattacks. That means investing in technology and ensuring that budgets for digital health projects include the costs of basic cybersecurity controls. Organizations should avoid unsupported software, which is more vulnerable to attack. In particular, investing in systems to identify attacks early is essential, as most attacks are only discovered months after they occur, when the damage is already done.

But while technologies to identify, protect, detect, respond and recover are crucial, they are insufficient — especially with the increasing use of artificial intelligence (AI). Our mindset must change radically to acknowledge that we cannot rely on information technology systems alone to protect us from cyberattacks. Therefore, enhancing cybermaturity also means investing in people. It is humans who perpetrate ransomware attacks, and it is humans who can stop them. Training staff to identify and respond to cyberattacks and rehearsing incident response plans are critical. Humans are both the weakest and strongest links in cybersecurity.

That is not something that any nation can do alone. Just as viruses do not respect borders, neither do cyberattacks. International cooperation is therefore essential. Many of the measures we take to address other threats are just as relevant here, whether collaborating on joint investigations and law enforcement, sharing intelligence or creating regional networks. WHO hosts two new global platforms for international dialogue: the Global Initiative on Digital Health and the Global Initiative on AI for Health — a tripartite platform with the International Telecommunication Union and the World Intellectual Property Organization.

My thanks again go to the Security Council for drawing attention to this very important issue. As members of the Council know, its mandate under the Charter of the United Nations is to maintain international peace and security. Cybercrime, including ransomware, poses a serious threat to international security. Just as members have used that mandate to adopt resolutions and decisions on matters of physical security, so we ask them to consider using that same mandate to strengthen global cybersecurity and accountability. WHO is committed to supporting all Member States to maximize the power of digital technologies for health and to minimize their risks.

The President: I thank Dr. Ghebreyesus for his briefing.

I now give the floor to Mr. Conrado.

Mr. Conrado: I thank you, Mr. President, for allowing me to participate in today's meeting. My name is Eduardo Conrado and I am the President of Ascension, the third-largest healthcare system in the United States.

Ascension is a non-profit and Catholic health system. We have about 330,000 people — including approximately 33,000 affiliated providers — working in our 120 hospitals, 2,000 ambulatory sites of care and 75 ambulatory surgery centres, which are located in 17 states and the District of Columbia. Each year we

provide care to more than 6 million individuals, with over 3 million emergency room visits, and perform nearly 600,000 surgeries. Ascension delivers roughly 1 in 50 of the babies born in the United States each year — to quantify that, it is between 72,000 and 78,000 babies annually. Our mission is to serve all with special attention and to provide compassionate and comprehensive care to those who are poor and vulnerable in the United States.

As members may know, the healthcare sector is particularly vulnerable to cyber and ransomware attacks because of its size and technological dependence and the sensitive data we secure and maintain. On 8 May, Ascension fell victim to a ransomware attack. The attack encrypted thousands of our computer systems and posed a significant challenge to our ability to serve our patients and communities. As a direct result of our systems being encrypted, we were not able to access our electronic health records. Several of our other technology systems were also unavailable, including those used by patients to communicate with their doctors and download their data. The ransomware attack also made it more challenging to access various systems used to order and perform certain critical diagnostic tests — such as laboratory tests, magnetic resonance imaging, computed tomography scans and X-rays — and to dispense medicines to our patients.

As soon as we discovered the ransomware attack, our healthcare teams initiated downtime procedures, which are pre-defined steps that all healthcare organizations follow during a system or network failure. One of those steps included switching to paper records while our electronic records were down. As members can imagine, that placed a tremendous burden on our dedicated workforce and clinicians. Let me paint a picture of what that looked like for our staff during that time.

Overnight, nurses were unable to quickly look up patient records from their computer stations. They were forced to comb through paper back-ups to find a patient's medical history or medications. Imaging teams were unable to quickly send the latest scans up to surgeons waiting in the operating rooms. Indeed, we had to rely on runners to deliver printed copies of the scans to the hands of our surgery teams. As we tried to bring on more staff to ease the burden on our nurses, we were hampered because our provisioning system was also offline. Due to the malicious attack, our care teams and our patients went from utilizing all of the incredible technology they use every day to working from paper, faxes and hand deliveries. In short, our modern care system was sent back in time.

During the attack, several of our hospitals were also forced to go on diversion for emergency medical services, which meant that ambulances were directed to other hospital emergency rooms instead of Ascension hospitals. The impacts of diversion can vary, but it can lead to delayed services due to increased travel times and potentially poor outcomes for patients. It can also create a ripple effect where receiving hospitals are overburdened and also forced to divert patients. In addition to diverting ambulances out of caution, some non-emergent elective procedures, tests and appointments were temporarily paused while we worked to bring our electronic systems back online.

Modern healthcare relies on many third-party digital solutions. We found that bringing those systems back online and convincing each of those hundreds of vendors to reconnect to Ascension was a monumental task. It took until 14 June, 37 days after the ransomware attack was launched, for us to restore connections and access to all our electronic health records and bring the last of our hospitals back online.

Today we continue to deal with the fallout of that attack. Now that our electronic health systems are operational again, we are undertaking the lengthy process of digitizing the data from all the paper patient records that were created and collected over those 37 days that our systems were down. To put it into perspective, the amount of paper generated in that period, if you stacked all the paper up, would be more than 1.5 kilometres high. It will probably take us until the end of this calendar year — a full six months since the reoperationalization of our systems — to be able to digitize those paper records.

While I have focused primarily on the impact of the ransomware attacks on our systems and services, I want to emphasize the tremendous human impact of such attacks. Our providers and staff rose to the incredible challenges from technology limitations and disrupted workflows to help provide patients the safe and effective care they needed. They did that while taking on longer hours, increased stress and, in some cases, increased burnout. In addition, when patients were diverted or sought treatment at other healthcare facilities, the providers and staff at those other facilities, too, had to shoulder an additional burden due to increased patient

volumes, limited access to medical records from Ascension and increased stress. We recognize the work those providers took on, and I want to thank them for their willingness and efforts to do so.

Our organization is just one of many healthcare entities targeted by cybercriminals every day. Unlike many smaller healthcare organizations that might not have as many resources as Ascension, we were fortunate to be able to quickly engage internal and external cybersecurity experts and legal counsel to investigate, contain the issue and secure our systems. We also worked closely with the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency in responding to the attack. Even still, the financial impact from the May 2024 ransomware attack was tremendous for us; Ascension has spent approximately $130 million on its response to the attack and has lost $900 million in operating revenue as of the end of this fiscal year.

Ascension is not alone in experiencing a significant financial impact from cyberattacks. Recent estimates suggest that the cumulative downtime costs, recovery efforts and lost revenue for United States healthcare organizations have reached more than $70 billion since 2019, and nearly $15 billion through October of this year alone. Ransomware attacks on healthcare systems have been increasing, with 386 healthcare cyberattacks reported so far in 2024 in the United States, according to the United States Department of Health and Human Services, and our incredible technology and cybersecurity teams inside Ascension stop attempts to attack our systems on a near-daily basis.

Ransomware attacks on the healthcare sector are more than cyberthreats — they can pose a direct and systematic risk to global public health and security. Such attacks are not driven by rogue individuals, but by professional cybercriminals who are highly skilled and well-resourced. International coordination and cooperation are needed to fight against ransomware attacks and safeguard healthcare systems worldwide.

We appreciate the Security Council's interest in protecting our healthcare systems and, ultimately, our patients and communities. I thank the members of the Council for their time this morning.

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

I shall now give the floor to those members of the Council who wish to make statements.

Mrs. Neuberger (United States of America): My name is Anne Neuberger, and since 2021 I have had the privilege of coordinating the United States national security policy on cyber and emerging technologies. I am honoured to represent President Biden today to speak about the threat of ransomware.

I would like to thank the United Kingdom for devoting part of its Security Council presidency to today's meeting and for its continued leadership on promoting responsible State behaviour in cyberspace. I also thank Dr. Tedros Ghebreyesus, Director-General of the World Health Organization, and Eduardo Conrado, President of Ascension Healthcare, for joining us. We appreciate the expertise and insights of their briefings.

Today I want to talk to the Council about three topics: first, the nature of the threat posed by ransomware attacks, particularly to healthcare systems; secondly, what the United States is doing to address that threat, both globally and at home; and finally, the critical role that every State can, and must, play in confronting the challenge.

The reality is that ransomware attacks on hospitals and healthcare systems are a serious threat to international peace and security. They jeopardize lives. They destabilize societies. The Security Council therefore has a role to play in countering that threat to peace and in spurring countries to action. Just a few months ago, at the Council's high-level open debate on evolving threats in cyberspace, convened by the Republic of Korea, Secretary-General António Guterres called on us to reflect on the immense benefits that digital technologies bring to our societies (see S/PV.9662). However, as the Secretary-General cautioned, the same connectivity that brings us together also exposes countries around the world to significant cyberthreats. Ransomware is one of the most pervasive and damaging of those threats. The United States Government is aware of more than 1,500 ransomware-related incidents in 2023 alone, generating more than $1.1 billion in ransom payments. That is a significant increase from 2022, when we saw a little more than half that much in ransomware payments. Indeed, the 2023 figure is a tenfold increase since 2018, and a 100-times increase since 2014.

And the United States is not alone. In July 2023, the port of Nagoya, Japan's business shipping port, was hit with a ransomware attack by the group LockBit, which forced the port to stop handling a large portion

of incoming shipping containers. That same year, a ransomware attack against a pathology partnership in the United Kingdom led to significant risk to the national blood supply. And South Africa's National Health Laboratory Service suffered a ransomware attack affecting the dissemination of lab results, hampering national efforts to respond to an outbreak of Mpox.

According to the United States intelligence community's June 2024 analysis, 51 per cent of global ransomware attacks in the first half of this year were against United States victims. The remaining 49 per cent are spread all across the world. That is truly a global threat. Healthcare and emergency services is one of the top four most targeted sectors for ransomware attacks, accounting for at least 191 incidents worldwide in the first half of this year alone. In the United States, our Federal Bureau of Investigation reported 249 reports of ransomware incidents against the healthcare sector last year.

What does a ransomware attack mean for a hospital? As we just heard from the briefing, it means ambulances diverted and other delays in emergency care, the cancellation of surgeries, delays to important medical treatments and breaches of extremely sensitive healthcare records. When directed at blood banks, ransomware attacks can prevent access to life-saving supplies. Ransomware targeting those facilities can result in major disruptions that jeopardize patient care and access to medications, increase the length of patient stays, force the transfer of patients to other facilities and cost lives. I want to re-emphasize that last sentence. Health experts have estimated that ransomware attacks were responsible for the deaths of dozens of patients in the United States Medicare systems between 2016 and 2021. More recent data confirms that mortality rates at hospitals increase when a hospital has been disrupted by cyberattacks.

What are we doing about this dangerous crime spree? We start from the premise that there is strength in numbers. We are not alone in facing this threat, and we are not alone in wanting to uphold international norms that prohibit all aspects of that behaviour. It was that belief that we could be more than the sum of our parts that inspired us in 2021 to launch the 68-member International Counter Ransomware Initiative, which includes a number of States that are around the table with me here today. That Initiative focuses on disrupting ransomware attacks, enhancing the security of critical infrastructure and increasing the capacity and incident-response capabilities of our partners together.

We are also using our own law enforcement capabilities to disrupt those crime waves. And to make ransomware attacks less appealing, we are working closely with cyberinsurers and the private sector to reduce ransomware payments and improve incident reporting. We have also pledged — along with 40 other States — not to allow our Governments or any of their agencies to pay ransomware bounties.

Beyond reducing ransom payments, we are engaged with public and private sector entities to halt the illicit flow of extorted ransomware payments, made in cryptocurrency, that is laundered through virtual asset service providers. And looking into the future, the United States Agency for International Development is working to establish a fund to build long-term cybersecurity capabilities against ransomware attacks and to help countries respond to and recover from ransomware attacks.

But none of us is doing enough. Ransomware attacks will continue, and perpetrators will thrive as long as ransoms are being paid and criminals can evade capture, particularly by fleeing across borders.

That brings me to my third and final topic — what can and should every country be doing to end this cycle of victimhood, plunder and impunity? And why should the Security Council, with its unique mandate, support efforts to tackle this evolving threat to peace and security?

Ransomware attacks are attractive to cybercriminals because of the large individual ransom payments. For a group like BlackCat, which has received more than $420 million in ransom payments since 2019, this is a thriving business. In fact, last year BlackCat and LockBit accounted for more than 30 per cent of claimed healthcare ransomware attacks worldwide. And in 2024, among other attacks, LockBit claimed credit for a cyberattack on Croatia's largest hospital and published confidential data on patients stolen from a French hospital system.

First, every State should act in accordance with the framework for responsible State behaviour in cyberspace, endorsed by the General Assembly repeatedly, and by consensus. By affirming that framework, we have already made commitments to address malicious cyberactivities emanating from

our territories. Under the framework, States should not knowingly allow their territory to be used for internationally wrongful acts using information and communications technologies (ICTs), and they should respond to appropriate requests to mitigate malicious ICT activity emanating from their territory aimed at the critical infrastructure of another State.

Therefore, when ransomware actors in one State target critical infrastructure like hospitals in another, it is incumbent on the first State to take action to investigate and mitigate that activity in line with the framework's norms, especially when they have been asked to do so. Yet some States — most notably Russia — continue to allow ransomware actors to operate from their territory with impunity, even after they have been asked to rein it in. The developer and administrator of the cybercriminal gang LockBit is Russian national Dmitry Khoroshev, whom our Department of Justice has charged for committing hacking crimes.

We assess cybercriminals affiliated with the most impactful ransomware variants, like the one that committed the attack against Ascension healthcare, are tied to Russia, based on members' citizenship, geographic location and claimed allegiance or association with known Russian cyberactors. Some money-launderers for those top ransomware actors are Russia-based and utilize Russian banks or cryptocurrency exchanges to launder their ill-gotten gains.

In 2021, President Biden met with President Putin and asked that he rein in ransomware attacks on United States targets. President Biden made clear in that meeting that, when a ransomware operation is coming from Russian soil, even when it is not sponsored by the State, the United States expects the Russian Government to act. Instead of adhering to its United Nations commitments, Russia continues to harbour those criminals. The United States implores States not to follow Russia's practice in protecting international cybercriminals and reiterates our request for States to follow the framework for responsible State behaviour in cyberspace as a matter of upholding international peace and security.

We issue today a call to action — countries that experience a ransomware attack against a hospital should inform the country of origin of the attack and request that they take action in line with their United Nations commitments regarding responsible State behaviour in cyberspace.

In conclusion, we can collectively eradicate this scourge if we act together, abide by our shared principles, refuse to pay criminal gangs and help each other to apprehend the cybercriminals who think they can outmanoeuvre our system. I thank members for their attention and look forward to continued and expanded cooperation in the days and months ahead.

Mr. Dharmadhikari (France) (*spoke in French*): I would like to begin by thanking the Director-General of the World Health Organization, Dr. Tedros Ghebreyesus, and Mr. Eduardo Conrado for their briefings, which clearly highlighted the issues at stake at today's Security Council meeting.

Last June, at the initiative of the South Korean presidency, the Security Council held an open debate on the evolution of cyberthreats (see S/PV.9662). Many States underscored the growing impact on international peace and security resulting from the misuse of information and communications technologies. Among the most severe threats are ransomware attacks. Ransomware threats continue to grow and to worsen. In 2023 in France, we saw a 30 per cent increase in those types of attacks over the previous year. That growth is prompted by the access on the market of source code and cyberintrusion tools, enabling numerous criminal actors to carry out cyberattacks.

Driven by financial motives, ransomware attacks have an impact on individuals, companies and on the very operation of essential public services, and hence on the stability of States. Some 10 per cent of ransomware attacks identified by French authorities in 2023 targeted healthcare establishments, with serious consequences for the delivery of vital care. Many attacks targeted enterprises in strategic sectors, research establishments, higher education institutions and public administrations.

As we know, ransomware attacks can help finance the proliferation of weapons of mass destruction. The most recent report by the Panel of Experts of the Security Council Committee established pursuant to resolution 1718 (2006) (see S/2024/215) pointed out that 40 per cent of North Korea's illegal nuclear and ballistic missile programmes were financed by cybercriminal activities.

In order to counter those threats, we must first reiterate our commitment to the norms that guarantee the security and stability of cyberspace. As the General Assembly has reaffirmed on a number of occasions,

international law, including the Charter of the United Nations, applies to cyberspace. States have defined, by consensus, a series of norms of responsible State behaviour in cyberspace, in order to improve the prevention and management of cyberincidents. That normative framework urges States to take every reasonable measure to prevent their territory from being used by malicious cyberactors to commit internationally wrongful acts. In the General Assembly, France will continue to support work aimed at promoting that normative framework, furthering a common understanding of it and supporting States in its implementation. France will participate actively in the coming year in discussions on establishing a permanent programme of action mechanism to meet those goals.

France supports and participates in the International Counter Ransomware Initiative, launched by the United States in 2021. The initiative fosters sharing best practices in order to craft a collective response to the threat posed by ransomware to our societies and democracies.

As a number of States stressed during the open debate held under the South Korean presidency in June (see S/PV.9662), within the framework of its mandate, the Security Council must also strengthen its grip on cybersecurity threats. Meetings like today's enable the Council to keep abreast of the changing cyberthreat landscape. France stands ready to work to improve understanding the stakes represented by cyberchallenges in the Council's subsidiary bodies, particularly when it comes to the circumvention of sanctions regimes.

Mr. Mikanagi (Japan): At the outset, I thank you, Sir, for convening this meeting following the request of seven Security Council members, including Japan. I also thank today's briefers for their insights.

It is significant that the Security Council is continuing to address threats posed by cyberattacks following the Arria Formula meeting and the open debate held in April and June (see S/PV.9662), respectively. Today we are witnessing increased risks of cyberattacks through ever-more sophisticated means. There is an upward trend of cyberattacks targeting critical infrastructure, including ransomware attack against healthcare facilities. The 2021 report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (see A/76/135) pointed out that complex and sophisticated uses of information and communications technologies (ICT) undermine trust, are potentially escalatory and can threaten international peace and security. The report also refers to the risks and consequences of malicious ICT activities during the coronavirus disease pandemic. Japan has continued to collaborate with Oxford University in examining the legal aspects of those issues through the Oxford Process on International Law Protections in Cyberspace and a report published last year on cyberoperations against the healthcare sector. Vulnerabilities in ICT constitute a risk factor for the whole world. No country can deal with the threat alone, and we need to work together with a sense of urgency.

Ransomware is one of the most disruptive cyberthreats undermining the operations of critical infrastructure in society, including hospitals and power plants. Given the overall impacts and ramifications, ransomware could certainly pose direct threats to international peace and security. Some Japanese hospitals have also experienced major impediments to their emergency-patient care and scheduled surgeries caused by ransomware attacks. Preventing a ransomware attack and, in the case of an attack, minimizing social and economic disruption are of the utmost importance. For those purposes, Japan values information-sharing and close cooperation among Member States' authorities, including law enforcement agencies; raising awareness for potential targets of ransomware attacks; enhancing cybersecurity resilience; and capacity-building. In that vein, developing collective resilience continues to be essential to preventing various actors from exploiting any vulnerability to ransomware attacks. Japan values and appreciates the United States-led Counter Ransomware Initiative and shares its firm commitment to working together at both the policy and operational levels to counter ransomware threats. Promoting capacity-building programmes to strengthen cybersecurity is also essential to ensure the safety and resilience of cyberinfrastructure. To that end, Japan has been providing capacity-building support to Indo-Pacific countries and will continue to do so in collaboration with like-minded countries, international organizations, industry and academia.

Japan reiterates the importance of the rule of law in cyberspace. Within the United Nations framework, we have been engaging in concrete discussions on the application of existing international law and implementing agreed norms, rules and principles of

responsible State behaviour. While we have agreed that existing international law applies to cyberoperations, we have also discovered that there is no agreement on the key issues, including violations of sovereignty and the application of the due diligence principle. In order to maintain peace and security while relying on cross-border data flows through the Internet, we must seek to strike an appropriate balance between the free flow of data and territorial sovereignty, as soon as possible. In our view, the current lack of agreement on those issues is not conducive to the maintenance of international peace and security. Therefore, we need to redouble our efforts in the search for common ground on the application of existing international law. To that end, the Security Council could also play a role. It might be difficult for the Council to determine the existence of a threat to international peace and security from a single cyberincident but, considering the worrisome trend of increases in malicious cyberoperations like ransomware attacks on the healthcare sector, the Security Council might be able to determine that certain trends of malicious cyberoperations pose a threat to international peace and security.

As we continue our work, Japan looks forward to contributing to the upcoming sessions of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies. Japan also believes that the programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security should serve as a future permanent platform to ensure a seamless transition from the OEWG after 2025. Lastly, Japan will continue to make efforts to fight against cyberthreats and pursue a free, fair and secure cyberspace.

Mr. Camilleri (Malta): We thank Dr. Ghebreyesus and Mr. Conrado for their insightful remarks.

The evolution of ransomware tactics represents a severe escalation in the cybersecurity threat landscape. Such attacks have become increasingly damaging, making recovery without succumbing to the demands of malign actors more challenging. That is why Malta joined the call for convening this meeting. The World Health Organization has identified ransomware as the primary digital threat to healthcare, a situation worsened by the coronavirus disease-driven digital transformation, The attacks do not only jeopardize access to essential medical services, but they also violate the fundamental right to privacy of the individual and threaten the overall well-being and security of citizens and their fundamental human rights.

The July annual progress report of the Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies highlights the growing concern among States regarding ransomware, noting the increased frequency and severity of the attacks. The rise of ransomware as a service has broadened the range of malicious actors involved. The report underscores the necessity for a comprehensive approach to counter the ransomware threat, which includes targeting the illicit financing of those activities. During the Security Council's high-level debate on cyberthreats during the presidency of the Republic of Korea in June (see S/PV.9662), several delegations recognized the potential of ransomware to destabilize Governments and disrupt essential public services. They also underscored the increasing intensity of ransomware and State-sponsored cyberattacks targeting critical infrastructure.

Those concerns were also underlined in the final report of the Panel of Experts of the Committee established pursuant to resolution 1874 (2009) (see S/2024/215), which reported on investigations of 58 suspected cyberattacks between 2017 and 2023, valued at approximately $3 billion. Reportedly, they help the Democratic People's Republic of Korea circumvent sanctions and continue develop weapons of mass destruction. Malta acknowledges the rapidly evolving nature of technology-driven threats and emphasizes the need for a comprehensive response. It is vital for Member States to ensure that the IT workforce, particularly in healthcare, possess up-to-date cybersecurity skills. In addition, raising awareness at the executive level about the potential of cyberattacks to serve as public health emergencies is crucial.

Investment in human capital, the establishment of robust incident-response processes and training clinical staff to maintain service quality during cyberattacks are essential. Developing strong communication pathways within healthcare entities for coordinated responses, potentially across borders, is also important. National efforts alone can only go so far. They must also be complemented by international cooperation to ensure adherence to international law. Cross-border ransomware attacks pose increasing risks to public health, with implications that extend far beyond mere technical disruptions. The availability of ransomware online has lowered the barriers for attacks, including by

transnational organized crime groups, making it easier for malicious actors to launch their operations globally.

Gender mainstreaming in cybernorm implementation and gender-sensitive capacity-building are needed. Women's involvement and participation in cyberdecision-making are crucial, especially in conflict and post-conflict contexts. Ensuring gender responsiveness in our cybersecurity strategies is essential for developing comprehensive and effective solutions.

In conclusion, we look forward to continuing our discussions on cybersecurity and commend the efforts made to highlight the vital role of the Security Council. We reaffirm our support for a programme of action guided by the United Nations. We believe that the agreed framework for responsible State behaviour in cyberspace is essential for fulfilling our shared responsibilities and aligning our common interests.

Mr. Hwang (Republic of Korea): I extend my gratitude to the World Health Organization Director-General and to Mr. Conrado for their valuable insights.

The Republic of Korea welcomes today's timely meeting on ransomware, one of the most significant types of cyberattacks. We are encouraged by the ongoing momentum in cybersecurity discussions at the Security Council this year, building upon the Arria Formula meeting in April and the signature event open debate in June (see S/PV.9662), over which the Republic of Korea presided during its Security Council presidency. During those meetings, many countries emphasized that, alongside other types of cyberthreats, ransomware has emerged as a critical challenge to international peace and security. Numerous countries have consistently emphasized the need for the Security Council to tackle cyberthreats, in accordance with its primary responsibility conferred by the Charter of the United Nations. In that regard, I would like to highlight the following points.

First, malicious cyberactivities, including ransomware attacks, act as threat multipliers, exacerbating existing challenges and amplifying conflicts. They disrupt essential social or public services, which can trigger social instability and undermine national security. In Ukraine, a number of cyberattacks on critical infrastructure, such as power grids and telecommunications systems, are causing widespread blackouts and network disruptions. They not only cause humanitarian suffering, but also further escalate the war.

Secondly, cyberattacks seriously undermine the Security Council's sanctions regimes. For example, according to the annual report by the Panel of Experts for the Committee established pursuant to resolution 1718 (2006) (see S/2024/215), the Democratic People's Republic of Korea generates approximately 50 per cent of its foreign currency revenue through malicious cyberactivities. That clearly underscores how cyberattacks have become a primary tool to circumvent and nullify Security Council sanctions. Furthermore, sanctioned armed groups are leveraging illegal cyberactivities to raise funds, conceal assets and trade weapons, complicating the enforcement of assets freezes and arms embargoes.

Thirdly, such illegal revenue is linked to the proliferation of weapons of mass destruction (WMD), which falls under the direct purview of the Security Council. Indeed, the Democratic People's Republic of Korea is funding 40 per cent of its illegal WMD and missile development programmes through malicious cyberactivities, as the most recent Panel of Experts report pointed out. Last week, the Democratic People's Republic of Korea launched a series of ballistic missiles, including a new type of intercontinental ballistic missile. Needless to say, North Korean information technology workers have also been engaging in serious crimes, such as the theft of intellectual property from numerous global defence firms, with the aim of advancing its WMD capabilities.

To cope with imminent threats posed by cyberattacks, including ransomware, we believe that it is urgent to enhance the role of the Security Council and strengthen international cooperation. At the Security Council level, we should consider requesting regular reports from the Secretary-General on evolving cyberthreats to mainstream cybersecurity into the Council's agenda and hold regular Security Council meetings as we do on other agenda items. In the mid-to-long term, we can take actions to pursue accountability in the Security Council in addressing cyberactivities that violate international law and harm international peace and security.

As for the need for international cooperation, we want to stress that cyberthreats are global, as evidenced by the recent incidents in Costa Rica and Trinidad and Tobago that took place over the past few

years, where ransomware attacks led to declarations of national emergencies.

The Republic of Korea also continues to be exposed to cyberattacks. As recently as this week, there was a distributed denial of service attack on the Ministry of National Defence. My Government announced a few hours ago that cyberattacks by pro-Russian hacking groups have increased following North Korea's troop deployment to Russia.

Given the transnational nature of cyberspace, our cybersecurity is only as strong as its weakest link. Therefore, international cooperation and capacity-building, particularly with the developing countries, are crucial in responding to cyberthreats. To that end, my Government is now participating in the Counter Ransomware Initiative led by the United States, which aims to enhance global awareness and build collective resilience against ransomware.

The Republic of Korea strongly believes that, in order to remain relevant, the Security Council should pay more attention to the threats emanating from emerging technologies, such as cyber and artificial intelligence. Along with our ongoing efforts, such as the adoption of the General Assembly draft resolution on AI in military domain at the First Committee this week (A/C.1/79/L.77) and the REAIM Summit 2024 in Seoul, the Republic of Korea will continue to play its part at the Security Council.

Mrs. Blokar Drobič (Slovenia): I would like to thank Director-General Ghebreyesus and Mr. Conrado for their valuable contributions to today's briefing.

Slovenia is a member of the Counter Ransomware Initiative. It is in that capacity that we would first like to draw the Council's attention to the most recent annual progress report from the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2015 (see A/79/214). In the report, the States Members of the United Nations expressed concern about the increasing scale and severity of ransomware attacks that disrupt essential services, including the healthcare sector, which is particularly dangerous and worrisome. Member States also highlighted that such attacks may have an impact on international peace and security and require a comprehensive response.

Our position on cyber-related discussions in the Chamber continues to be guided by the Council's primary responsibility to maintain international peace and security. Due to the very unique character of cyberspace, the issue is international and only seldom confined by national borders. It is therefore a problem that can be solved only with a high degree of international cooperation. To fulfil that responsibility, the Council must actively engage in addressing the threats posed by ransomware attacks, including on hospitals and other healthcare facilities and services.

Following the coronavirus disease pandemic and the rapid digital transformation of healthcare organizations globally, ransomware attacks have increasingly targeted those entities. State and non-State actors are incentivized to exploit critical healthcare information technology systems or compromise the confidentiality of personal data and data concerning health. In many instances, non-State actors are sheltered, or even facilitated by, Governments. Ransomware attacks on health facilities and institutions create a direct threat to public health, safety and security.

Because of such attacks, diagnostic imaging, pathology, emergency departments, ambulance services and cancer care have all been consistently disrupted. This is not a victimless crime; human lives are endangered. The impacts of such attacks of course have also been financial, with a ransomware attack on one Member State's healthcare system estimated to have cost around $100 million. That money can be used to fund other crimes and potentially even terrorism.

Given the rapid development of artificial intelligence, which has even further accelerated the conduct of ransomware attacks, allowing both State and non-State actors to carry out such attacks without requiring high technological skills, a decisive response by the international community is needed to prevent and mitigate their impact. Capacity-building, particularly on a technical level, is fundamental to increase cyber-resilience. In that vein, Slovenia co-founded the regional Western Balkans Cyber Capacity Centre and its training for trainers programme, which has been successfully executing regional training in the Western Balkans for the past year and a half.

As the majority of ransomware attacks are cross-border in nature, the Council should play a decisive role in de-escalating tensions and promoting accountability, especially when such attacks endanger security and even lives. We also believe that the Council could

consider designating cybercriminals to be listed under sanctions regimes.

Allow me to conclude by assuring fellow Council members of our unwavering commitment to collaborate with them and with the broader United Nations membership to continue discussions on ransomware threats, which are a shared concern when it comes to international peace and security. We also remain steadfast in our commitment to continue to implement measures aimed at mitigating those risks, including by implementing the existing norms of responsible State behaviour in cyberspace.

Mr. Nebenzia (Russian Federation) (*spoke in Russian*): We would like to thank Dr. Tedros Ghebreyesus, Director-General of the World Health Organization, for his briefing. We listened attentively to Mr. Eduardo Conrado, President of the non-profit organization Ascension.

All members of the international community are acutely aware of the attention afforded by the Russian Federation to issues of security concerning the use of information and communications technologies (ICTs). It was our country, over a quarter of a century ago, that initiated discussions on the matter within the United Nations. Russia was behind the idea of creating specialized negotiating formats within the United Nations, including the current successful Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021–2025. We also initiated the work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, wherein a draft document was successfully agreed in August (see A/AC.291/22/Rev.2).

There are various inclusive thematic mechanisms for discussing issues pertaining to information security, including a broad range of existing and potential threats in that area. Therefore, it remains unclear to us what prompted the need to further expand the discussion into the Security Council. We have not heard a concrete answer to that question today. Furthermore, given that today's event was requested within a very short time frame, we have not been able to understand from the statements of its initiators what constitutes the immediate and specific threat posed to international peace and security. It is precisely such situations that the Security Council must prioritize, based on its mandate.

Given the focus of today's meeting on the issue of ransomware, we would like to note that the draft United Nations Convention against Cybercrime, to which I referred, is designed to combat the use of that type of malicious software on an equal footing with other types of ICT-related offences that are no less serious for public and personal safety. We urge all of our colleagues to focus on facilitating the swift entry into force of that important practical international treaty. Moreover, in the light of the ever-expanding range of cybercrime threats, we should already be considering further developing the Convention by adopting additional protocols thereto.

With regard to ensuring the protection of critical infrastructure, including healthcare facilities, from malicious uses of ICTs, Russia is fully versed in such risks. Our country regularly faces cyberattacks on healthcare facilities. Since the beginning of 2022, we have repeatedly experienced incidents of varying nature and scale — from the theft of patients' personal data and the disabling of a computed tomography scanner to the hacking of children's hospitals' websites, causing them to crash. In many cases, Ukrainian groups — in particular the NATO-backed IT Army of Ukraine — are responsible for such attacks.

We should like to recall that the consensus understanding on the need to ensure the security of facilities providing vital services to the population has been repeatedly confirmed within the framework of the work of Groups of Governmental Experts and OEWGs on international ICT security. The relevant norms were also developed there. We are convinced that the greatest contribution to strengthening the security of critical infrastructure would be the codification of the relevant arrangements, which are currently voluntary and non-binding in nature.

To that end, we favour the swift elaboration of an international legal instrument that would cover all aspects of ensuring security in the use of ICTs. The most appropriate platform for efforts in this area would be a permanent negotiating mechanism under the auspices of the United Nations, which would be established at the end of the mandate of the current OEWG in 2025. Indeed, just the day before yesterday, the First Committee of the General Assembly adopted by consensus a draft resolution introduced by Singapore that enshrines that agreement (A/C.1/79/L.13).

Returning to our doubts about the added value of today's meeting, we believe it is important to bear in mind that the consideration in the Security Council of the issues of malicious use of ICTs, especially pertaining to specific incidents, is complicated by the specific characteristics of cyberspace. We are talking, first and foremost, about its anonymity, which makes it virtually impossible to reliably identify the source of malicious activity. Against that background, any attempts to resort to so-called political attribution are extremely unconstructive and even dangerous — in fact, it conceals a hackneyed desire to reserve the right to make groundless and politicized accusations against unfavourable States, of course without providing any evidence whatsoever.

Unfortunately, today's meeting was no exception to that rule. Once again, the United States has decided to use the Security Council's platform to promote its narrative, which is divorced from reality. The speculation about so-called Russian hackers and insinuations about our country's alleged encouragement of malicious activities in the use of ICTs have long sounded like a joke, which any sensible person would only smile at.

Nevertheless, Washington persists in resorting to such rhetoric, apparently appealing mainly to a domestic audience. Even during Tuesday's presidential election in the United States, the theory of notorious Russian interference was periodically thrown into the public space, despite the fact that the United States own Cybersecurity and Infrastructure Security Agency stated that there were no attempts to maliciously influence the results. Yet the United States and its allies continue to actively use rhetoric about an imaginary cyberthreat from their political opponents. The groundlessness of such insinuations has been repeatedly clarified by us within the relevant forums.

We would like to recall that, within the framework of the discussion under the auspices of the General Assembly, practical measures have been developed to strengthen depoliticized cooperation among United Nations States Members in the field of information security, including with regard to responding to cyberattacks. I am referring first and foremost to the global intergovernmental points of contact directory, which was launched in May on the initiative of the Russian Federation. That mechanism is aimed at preventing and resolving serious incidents in cyberspace, as well as reducing tensions in crisis situations. In the event of a serious episode of the malicious use of ICTs, any State can use that tool. It is indicative that we have not received any requests through the registry from those countries that so zealously accuse Russia of conducting cyberattacks. That once again demonstrates that the United States and its allies have no technical evidence to back up their findings.

At the same time, Washington itself does not hesitate to acknowledge the facts of its own operations conducted against Russia with the use of ICTs, as well as the build-up of its offensive capabilities in that area. Moreover, American intelligence services are widely practising so-called false flag operations. They are doing so even against their closest allies, who are so active in their support for the United States in promoting its aggressive policies.

Given the considerations outlined, we believe that today's meeting can hardly be deemed a rational use of the Council's time and resources. Our discussion essentially boils down to trotting out well-known national positions and duplicating the work conducted under the auspices of the General Assembly. If our Western colleagues wish to discuss the security of healthcare facilities, do they not think that what we should start with is not the threats emanating from cyberspace, but the need for the Security Council to agree on concrete steps to stop the horrific, senseless attacks by Israel on hospitals in the Gaza Strip, which are killing thousands of people? Until that happens in the real world, shifting the Council's attention to the virtual world seems counterproductive and even cynical.

We call on all constructive-minded States to continue their active participation in the global discussion on international ICT security. Our country remains strongly committed to continuing dialogue with the entire international community with a view to creating a peaceful and safe cyberspace, including through the development of legally binding agreements in that area within the framework of specialized inclusive mechanisms under the auspices of the General Assembly. We hope that such cooperation will enable us all to respond effectively and collectively to any threats in that area.

Mr. Geng Shuang (China) (*spoke in Chinese*): I thank Dr. Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization, and Mr. Eduardo Conrado for their briefings.

We live in a rapidly changing cyber-age. While fully enjoying the development opportunities from

cyberspace, we are also faced with complex and diverse cybersecurity challenges. Cyberattacks, cybercrime and cyberterrorism are increasingly becoming global menaces, and ransomware is a prominent issue in that regard. The issue of ransomware is highly specialized and technical. It is essentially a cybercrime. China is not in favour of the hasty push by the relevant Security Council members to discuss this issue in the Council and hopes that all parties can engage in more specialized, practical and in-depth discussions in other more appropriate platforms.

Just now, the briefers and some members listed examples of ransomware attacks in their statements. China supports the international community's efforts to analyse and address the multiple dimensions of this issue, such as the sources of ransomware, the pathways for its spread and its channels for monetization. We believe that countries should step up information-sharing, technical law enforcement and judicial cooperation in a joint effort to respond.

Ransomware is just one of the many challenges to cybersecurity. Other types of cyberattacks, such as phishing, cloud-system intrusion, theft of personal data and distributed denial-of-service attacks are also growing rapidly, with the modus operandi of cybercrimes becoming more diverse and systematic. China supports strengthening cybersecurity governance and maintaining lasting peace and stability in cyberspace. To that end, we call on all parties to make efforts in the following areas.

First, we should firmly uphold the peaceful nature of cyberspace. We should oppose wrong practices such as defining cyberspace as a domain for military operations, making rules of engagement in cyberspace, building cybermilitary alliances and listing the critical infrastructure of other countries as targets for cyberattacks. We reject the militarization of, and an arms race in, cyberspace with a view to fundamentally curbing the development and proliferation of offensive cybertechnologies, including ransomware.

Secondly, we should uphold the role of the United Nations as the main channel. On the basis of broad and equal participation, we should formulate international rules on cyberspace that are generally acceptable to all parties, abandon the small circles drawn along ideological lines, build a multilateral, transparent and democratic global governance system and jointly safeguard the cybersecurity of all countries.

Thirdly, we should adhere to bilateral and multilateral cooperation to combat cybercrime and cyberterrorism. We should comprehensively combat the entire chains of unlawful acts in that regard and further improve the law enforcement and judicial assistance mechanisms of all countries. In that regard, China welcomes the agreement reached by the United Nations in August to adopt the Convention Against Cybercrime.

Fourthly, we should step up assistance to developing countries to build capacity for maintaining cybersecurity. We should actively engage in international cooperation in areas such as talent cultivation, technological innovation, early warning and prevention and emergency response; shore up the weak links in global cybersecurity; leave no country behind; and allow no part of cyberspace to become a lawless space.

Cyberspace affects peace and security and people's livelihoods and well-being. China stands ready to work with the international community to jointly explore responses to cybersecurity threats and challenges and to make tireless efforts to uphold prosperity and stability in the global cyberspace and build a community with a shared future in cyberspace.

Mr. Afonso (Mozambique): Mozambique commends the United Kingdom presidency for bringing to the Security Council's attention such a timely and critical topic. We are grateful to today's briefers, namely, Dr. Tedros Adhanom Ghebreyesus, Director-General of the World Health Organization, and Mr. Eduardo Conrado, President of Ascension, for their very important and insightful briefings.

Ransomware has emerged as a preferred tool for cybercriminals and terrorist networks. It is a criminal activity that has especially severe consequences for countries lacking advanced cybersecurity resources. As we heard from the briefers, the healthcare sector is particularly vulnerable to such attacks, especially in developing countries, where reliance on digital systems for essential services such as electronic health records and diagnostics is growing but often without the necessary security measures in place. In our countries, disruptions such as those we heard about today can be catastrophic, not only threatening patient safety but also risking human lives. The impact on nations with fewer resources to respond is exponentially greater. In developing countries, ransomware represents a clear and present danger to our national security and

to the stability of essential public services, economic resilience and public trust in governance. Furthermore, cross-border attacks exacerbate geopolitical tensions, putting developing countries at risk. Those attacks can cause collateral damage in broader cyberconflicts.

Emerging technologies such as Artificial Intelligence and quantum computing amplify that threat. They intensify the challenge for countries with limited access to advanced cyberdefence capabilities and are pushing the world towards a digital arms race. In that connection, developing nations as such Mozambique face particular vulnerabilities. Those are due to limited cybersecurity infrastructure, underdeveloped regulatory frameworks and a lack of access to high-quality digital security training. When ransomware attacks disrupt critical sectors such as healthcare, recovery requires significant financial resources for expert intervention, system upgrades and, at times, ransom payments. For countries with already strained budgets, those demands present a nearly impossible challenge.

For those reasons, we believe that addressing ransomware in developing countries requires a comprehensive and tailored strategy. That approach must emphasize prevention above all. It must also encompass preparedness and response, including training information technology staff, modernizing outdated systems and establishing robust regulatory policies and partnerships. Preventive measures — such as regular software updates, network segmentation, zero-trust architecture and employee training on phishing awareness — are essential, but such measures often require capacity-building support.

Mindful of the negative impact that ransomware has on countries' economies, Mozambique has been developing a regulatory framework to tackle that problem and cybercrime in general. As part of those actions, we can highlight the drafting of a cybercrime law, a data protection law and a cybersecurity law. In addition to the legislative aspects, Mozambique has been implementing mechanisms to strengthen cybersecurity and resilience, with an emphasis on awareness and training at various levels.

On the global level, we call for a focus on creating unified cybersecurity standards and improved enforcement. No country should become a safe haven for cybercriminals. More important, we consider that a global and robust legal framework is urgently needed and should be fully in line with the purposes and principles of the Charter of the United Nations.

We hope that today's dialogue will serve as a step towards enhanced international cooperation and diplomatic engagement to deter and respond to cyberthreats. Strengthening those efforts is critical to safeguarding global peace and security and ensuring that no nation is left behind and unprotected in this digital era. As in other situations that are a threat to international peace and security, we must also join our efforts to make cyberspace secure and resilient.

Mr. Hauri (Switzerland) (*spoke in French*): I would like to thank Dr. Tedros Ghebreyesus, Director-General of the World Health Organization, and Mr. Conrado for their detailed contributions.

Switzerland welcomes the Security Council's renewed focus on the important issue of cybersecurity. Threats in cyberspace, particularly those emanating from State actors or tolerated by States, can threaten international peace and security, as recognized in the Pact for the Future (General Assembly resolution 79/1).

The many opportunities offered by developments in information and communications technology (ICT) are undeniable. The diversity of dangers and State and non-State actors that exploit the vulnerabilities of systems to carry out malicious cyberattacks is just as well known. Among them, ransomware attacks against healthcare systems are an extremely worrisome trend that has been increasing globally since 2020.

The digitization of healthcare systems is enabling great progress to be made for the benefit of the population, but its cyberinfrastructure is becoming increasingly complex and therefore more costly to secure. The need to remain operational at all times increases the pressure on healthcare providers themselves, as well as on public bodies. Such attacks are therefore a particularly perfidious way of targeting a State's critical infrastructure and sovereignty.

Recent reports of collaboration between a group sponsored by the Democratic People's Republic of Korea and the Play ransomware network raise serious security concerns, as it could lead to more widespread and damaging attacks on a global scale.

Let me highlight three aspects.

First, we reiterate that international law, including the Charter of the United Nations, international

conventions on human rights and, in the event of armed conflict, international humanitarian law, also applies and must be respected in cyberspace. In particular, the principle of due diligence, which has developed over a long period, and, in Switzerland's view, forms part of customary international law, calls on all States not to knowingly allow their territory to be used for actions contrary to the rights of other States. That applies to both the physical world and cyberspace. States are called upon to exercise due diligence to prevent criminal groups from using their ICT infrastructure, and to cooperate nationally and internationally to impede the activities of such groups. That principle is also recognized in the framework of responsible State behaviour in cyberspace, adopted by consensus. These standards also require states not to knowingly conduct or support cyber operations against critical infrastructures, such as health services.

Secondly, the repression of criminal groups active in cyberspace is important. Recent police actions have had a considerable effect on those groups, but their repression alone will not eradicate the phenomenon. States must act and take appropriate measures to prevent attacks on their critical infrastructure. We attach particular importance to strengthening the resilience and security of the healthcare sector in the field of cybersecurity.

Thirdly, in this often-transnational context, we can succeed only by working together. International cooperation and capacity-building among all States must be encouraged to increase the resilience and security of the global cyber-ecosystem. The International Counter Ransomware Initiative, of which Switzerland is a member, is an important forum in that respect. States must also comply more fully with their international obligations regarding requests for mutual legal assistance, so that criminal proceedings can take place wherever the perpetrator is identified.

At the multilateral level, I would like to stress the importance of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. Next year, it will be important for the Group to be able to recommend the establishment of a single mechanism within the General Assembly to continue its work, building on the achievements of recent years.

"Navigate Uncertainty, Strengthen Humanity" was the theme of the thirty-fourth International Conference of the Red Cross and Red Crescent. One of the resolutions adopted under that theme emphasized the importance of international humanitarian law in protecting the civilian population and civilian property in the context of armed conflict in the digital world.

The Security Council also has a role to play. It must promote respect for international law and the implementation of the framework of responsible State behaviour in cyberspace so that our populations can benefit from the vast opportunities offered by cyberspace, particularly in the field of health.

Mr. Koudri (Algeria) (*spoke in Arabic*): At the outset, I would like to thank Dr. Tedros Ghebreyesus for his valuable briefing. I also listened carefully to Mr. Conrado's briefing.

The surge in ransomware attacks against medical facilities is being amplified by the rapid emergence and exponential development of hacking software and artificial intelligence (AI). The risks are being magnified by the lack of international regulatory norms in that domain.

The recent successful conclusion of the United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, led by Algeria, demonstrates what we can achieve through genuine multilateral cooperation.

Two key principles are paramount.

First, the current approach to cybersecurity, including healthcare cybersecurity, continues to perpetuate global inequalities and exacerbates vulnerabilities to threats enhanced by AI.

Secondly, solutions must emerge from inclusive, multilateral processes that respect the sovereignty and sovereign equality of all nations.

Accordingly, it has become necessary to address five fundamental challenges.

First, we must address technological hegemony, in which developed countries, private companies and even individuals monopolize cybersecurity capabilities and AI technologies, leaving healthcare systems vulnerable in development countries.

Secondly, we must address the challenge of unilateral action, in which the domination of cyberspace and AI development, through technological barriers, continue to undermine international cooperation.

Thirdly, we must address the challenge of resource disparity, in which developing countries must struggle to protect their healthcare infrastructure against the backdrop of limited access to technology and expertise.

Fourthly, we must address the challenge of uncertainty, in which AI tools, while offering immense potential for development, defence and security, can be misused to enhance the sophistication and scale of attacks, including against healthcare facilities, instead of protecting them.

Fifthly, we must address the challenge of overlapping threats, in which ransomware attacks are not the only danger against personal data. The opaque and sophisticated business of data is equally a threat to personal data and privacy rights.

Those patterns of hegemony, non-inclusivity, disparity, uncertainty and AI chaos are all interconnected.

In that context, we underline three concrete measures.

First, we must establish international mechanisms for technology transfer and capacity-building, ensuring universal access to cybersecurity solutions for civilian facilities.

Secondly, we must develop standardized, but adaptable, cybersecurity protocols that work for nations at different development stages, recognizing that one-size-fits-all approaches are ineffective.

Thirdly, we must create affordable security solutions tailored to the needs of healthcare systems in developing countries. The international community must prioritize putting ethics first in AI development.

Furthermore, we must commit to safety and controllability. There are many uncertainties in the development and application of AI-related technologies, and safety is the bottom line that must be upheld. The international community needs to enhance risk awareness, establish effective risk warning and response mechanisms and eliminate controllable risks.

We stress that the concerns of the States of the South must be central, not peripheral, to international cybersecurity and AI frameworks. That is not just about fairness; it is about effectiveness. The healthcare systems of developing nations often face unique cybersecurity challenges, which require tailored solutions, rather than imposed standards.

In conclusion, the path forward in this domain requires both immediate and long-term measures through inclusive multilateral processes, with all actors working together on an equal footing, as demonstrated by the success of the Convention on Cybercrime.

The world should move towards more technological equality and shared capabilities, more multilateral cooperation, less unilateral action, fewer imposed solutions and more inclusive approaches. It should move towards AI development that serves humankind, rather than endangers it.

The safety of our healthcare systems is not a privilege for wealthy nations. It is a fundamental right that must be protected and provided to all peoples of all nations. We should work together to ensure that technological advancements in healthcare cybersecurity and AI do not become another factor in widening global inequalities.

Mr. Kanu (Sierra Leone): I thank Dr. Tedros Ghebreyesus, Director-General of the World Health Organization, for his informative briefing and Mr. Eduardo Conrado, President of Ascension, for the information provided.

Sierra Leone has prioritized addressing new and emerging threats to international peace and security in our tenure on the Security Council. We therefore welcome the opportunity to address this important issue regarding the rising threat of ransomware attacks against hospitals, healthcare facilities and services, which has the potential to undermine the fundamental right to health and threatens the global fight against public health crises.

Sierra Leone stands firm in recognizing that cyberattacks, including ransomware attacks, pose a growing challenge to international peace and security, particularly when they target critical infrastructure, like healthcare systems. These attacks not only cause widespread disruption, but also put lives at risk, affecting the most vulnerable, particularly in conflict zones, underresourced settings and during health emergencies, such as pandemics.

Whether perpetuated for financial gains and/or sociopolitical disruption, cyberattacks on healthcare systems, especially ransomware, have been opportunistic in preying on our reliance on digital health interventions, including Internet-connected telemedicine, eHealth, virtual communication platforms and health systems management dashboards,

particularly since the coronavirus disease pandemic, which ushered in an increased demand on healthcare systems. They also militate against increase access to healthcare and health systems. While reliance on Internet-connected and computer-based healthcare systems makes healthcare management much more efficient and effective, it also increases vulnerability to cyberattacks by criminal organizations. Such organizations exploit and profit from those facilities, which provide life-saving services but which also store large volumes of sensitive and personal data.

While ransomware attack claims have increased worldwide across all sectors, reports from the World Health Organization, INTERPOL and the intelligence services of some Member States indicate that attacks on the healthcare industry are particularly insidious. Several healthcare cyberattacks have been reported in the first half of 2024. INTERPOL's *African Cyberthreat Assessment Report 2024* states that nearly half of the African countries surveyed reported ransomware attacks against their critical infrastructure, including hospitals. Added to that are several countries' reports in recent years of having experienced attacks on their healthcare infrastructure, leading to loss of patient data, to the disruption of essential health services and even to deaths. Those attacks are not just criminal in nature, but they also represent a clear and present danger to public health, which is intrinsically linked to international peace and security.

In line with African Union and regional efforts, Sierra Leone strongly supports the need for a concerted international approach to combat cybercrime and strengthen the resilience of our health systems. The 2020 African Union Convention on Cybersecurity and Personal Data Protection emphasizes the need for collaboration, capacity-building and knowledge-sharing among member States to prevent and respond to cyberthreats. Sierra Leone is committed to aligning with that framework and working with the African Union and the wider international community to enhance the cybersecurity capabilities of African States.

We must also acknowledge the importance of multilateral engagement in addressing those challenges. The United Nations, through its various bodies, including the Office of Counter-Terrorism and the International Telecommunication Union, is to play an essential role in providing a platform for cooperation, facilitating technical assistance and fostering the development of international norms for responsible State behaviour in cyberspace. The recent call in the Global Digital Compact (see General Assembly resolution 79/1) to ensure a secure, inclusive and sustainable digital future must be seen as a critical opportunity to promote global cooperation on cybersecurity. Sierra Leone supports the principles laid out in the Compact, which include ensuring access to a secure and resilient digital infrastructure, safeguarding critical services and promoting the responsible use of technology by all actors, including private and non-State actors, who often play a role in those attacks.

In noting the increasing levels of ransomware attacks on healthcare operations and facilities worldwide, we highlight three main points.

First, Sierra Leone, as already noted, recognizes that ransomware attacks on hospitals and other healthcare operations are a threat to national security and to international peace, security and development. Access to quality healthcare is an essential need for people all over the world, and cyberattacks that disrupt the provision of those services endanger public health, putting the lives and livelihoods of millions of people at risk and potentially exacerbating insecurity and conflict. There are harrowing accounts of the chaos caused by ransomware attacks across the world in the recent past, and we have heard Mr. Conrado's account.

In a world in which most tertiary healthcare facilities have become partially or fully digital, the loss of those systems severely challenges effective patient care. The implications for global health and security become even higher when we consider attacks on global health institutions and medical research centres that support healthcare services for a large percentage of the world's population and that conduct medical research with biological toxins or infectious agents, which could be easily exploited by terrorist and criminal organizations.

Secondly, the transboundary nature of cyberattacks, including ransomware attacks, whose perpetrators often remain borderless, faceless and nameless and whose victims are spread across geographical lines, requires collaboration and coordination at the international level. At the regional level, we urgently call for support for the implementation of the African Union's cybersecurity initiatives, while fostering a regional approach to ensure that the continent's health infrastructure is protected from digital threats.

As cybercriminals become more organized, use more sophisticated malware and conduct more targeted

attacks, such as attacks on medical devices instead of on medical networks and systems, it is imperative that our efforts to combat that threat combine viable and appropriate legislative, intelligence and law enforcement measures. Strong actions taken at the national level must be underpinned by global treaties, laws and regulations that not only establish norms of conduct, but are backed by meaningful consequences for violators, thereby ensuring that cybersecurity threats targeting hospitals and healthcare facilities are treated as a serious matter of international peace and security, with an emphasis on collective action, accountability and deterrence.

As a member of the International Counter Ransomware Initiative, Sierra Leone remains committed to strengthening our national response systems against cybercrime through such legislation as the Cybersecurity and Crime Act, which we enacted in 2021. As a signatory to the Council of Europe Convention on Cybercrime, we welcome the approval this past August of the United Nations Convention against Cybercrime by the Ad Hoc Committee established by the General Assembly, which, according to the United Nations Office on Drugs and Crime, is

> "a landmark step as the first multilateral anti-crime treaty in over 20 years and the first United Nations Convention against Cybercrime at a time when threats in cyberspace are growing rapidly".

Thirdly and finally, in recent years, the Security Council has been instrumental in supporting countries and institutions to develop responses to this threat, including by shining a spotlight on it and increasing the global community's knowledge base for informed decision-making. Information-sharing on threats and perpetrators, along with the development and use of preventive security measures, including with the private sector, as appropriate, are key to the defence of public health and safety. It is also important that the Council ensure adherence to established rules, norms and principles regulating the responsible use of cyberspace.

Given that there are significant gaps among countries in harnessing the requisite financial, logistical and human resources capacities to adequately respond to cyberattacks, global and regional collaborative mechanisms must include enhanced cooperation on capacity-building, including the sharing of technology and expertise, especially for small and developing countries, in order to deepen their understanding of those threats and to implement measures to counter them.

In conclusion, Sierra Leone is of the firm view that the response of a strong and unified Council to the threat posed by ransomware attacks on hospitals, healthcare operations and facilities is key in establishing a peaceful and secure cyberspace. We reiterate our support for initiatives in that regard, within the context of established norms and principles for responsible State behaviour, human rights and the fundamental principles of the Charter of the United Nations.

Ms. Persaud (Guyana): At the outset, I thank World Health Organization Director-General Ghebreyesus and Mr. Conrado for their briefings.

Recent statistics reveal startling increases in the frequency and scale of ransomware attacks worldwide. Attacks against critical infrastructure, particularly hospitals and healthcare facilities, are having serious ramifications for public health and national security. The risks of such attacks are increasing as more health systems globally are using digital transformation to enhance the clinical quality and the cost efficiency of their services.

With greater access to ransomware and the broadening of threat actors worldwide, we are seeing an increase in the scale of ransomware attacks against medical institutions, negatively affecting their operations and the provision of healthcare services, in addition to resulting in the theft of confidential data. In addition to disrupting the delivery of health services and the financial implications due to downtime, ransomware attacks have in some instances resulted in the loss of lives, when the delivery of urgent medical treatment was compromised.

Given its potentially debilitating effects on the stability of national healthcare systems, the development of robust frameworks to counter such attacks must be a priority. States must act more urgently to adopt a proactive and holistic approach to addressing such attacks, while recognizing that they transcend borders and that no country is immune. In that context, I highlight the following points.

First, States must invest in capacity-building initiatives and develop incident response plans. Many developing countries lack the necessary resources and expertise to protect themselves from and combat cyberthreats such as ransomware attacks. As such,

building capacities in those countries is critical. That should include technical assistance, funding support and training to enhance the response capability of vulnerable States, including in the development of incident response plans to deal effectively with those attacks.

Secondly, given the growing magnitude and consequences of ransomware attacks, Guyana underscores the need to foster cooperation between and among States through knowledge-sharing on best practices and challenges, information exchanges and technology transfers. In that regard, it is vital to establish an international information-sharing system that provides information to countries on how they can strengthen and protect their critical health infrastructure from being vulnerable to ransomware attacks, so that they can be detected and addressed in time. In addition, a global framework must be developed that caters for this type of intelligence-sharing among States and relevant stakeholders on potential cyberthreats.

Thirdly, the perpetrators of ransomware attacks must be held accountable. Priority must be given to collaboration and partnerships to investigate and prosecute cybercrimes, inclusive of ransomware attacks across countries and regions. That should involve the dismantling of ransomware networks and monitoring of transactions suspected to be ransomware payments. The recently adopted United Nations Convention against Cybercrime contributes to that effort by providing regulatory and cooperative frameworks to address such crimes. In addition, Guyana recognizes that international law is applicable to cyberspace.

Hospitals, healthcare facilities and services should be treated as sacred, and all efforts must be made to protect them from ransomware attacks. The international community must join forces to prevent all forms of cyberattacks on critical national infrastructure. Guyana remains committed to global initiatives that seek to raise awareness of and address this threat and to ensure that it does not undermine international peace and security.

Mr. Montalvo Sosa (Ecuador) (*spoke in Spanish*): I would like to thank the Director-General of the World Health Organization, Dr. Tedros Adhanom Ghebreyesus, for his important briefing. My delegation would also like to thank Mr. Eduardo Conrado — we paid careful attention to his briefing.

Ransomware attacks against the health sector not only put the integrity of health systems at risk, but they also threaten human lives. By disrupting critical services and limiting access to essential medical services, those attacks affect public health, and they therefore pose a threat to international peace and security. The third annual progress report of the Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, dated July 2024, highlights the growing concern of States about the frequency, scale and severity of such attacks, which are increasing. As my delegation stated during the open debate held last June at the initiative of the Republic of Korea (see S/PV.9662), the Security Council must not lag behind with regard to the evolving cyberthreats.

As we have said on several occasions, Ecuador considers prevention to be the cornerstone of peacebuilding. In that vein, among its products, the Security Council should include capacity-building on harnessing technologies and strategies to combat their malicious use, complementing global efforts.

If one Member State is not safe, no Member State is safe. The threats we face today are, to a greater extent, transnational in nature, and the only way to counter them, both in the physical realm and in cyberspace, is through international cooperation. Cybersecurity is a global challenge that requires a comprehensive, coordinated and cooperative response from the entire international community. Therefore, my delegation supports any mechanism that favours greater international cooperation to reduce asymmetries in the capacity to implement rules for responsible behaviour by States, as well as the adoption of measures that strengthen the capacity of nations to protect their critical infrastructure. Existing norms need to be strengthened to take account of rapid technological developments.

Ecuador reaffirms its commitment to a secure, open and peaceful cyberspace, where technology can serve as a tool for development. All States have an obligation to strengthen multilateralism in order to build a digital environment that respects human dignity, by promoting international peace and security. International law and international humanitarian law are applicable to cyberspace.

I conclude recalling the need to preserve and promote the responsible use of information and communications technologies as the key to ensuring stability and security in cyberspace.

The President: I shall now make a statement in my capacity as the representative of the United Kingdom.

I would like to thank Dr. Ghebreyesus and Mr. Conrado for briefing us today.

Earlier this year in the General Assembly Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, all States recognized that ransomware attacks may have an impact on international peace and security. Ransomware actors have consistently attacked critical national infrastructure, local government and hospitals for personal financial gain. Most groups exist in jurisdictions that allow them to operate with impunity. We call on those States to do more to tackle the criminal groups based in, or making use of, their territory.

The United Kingdom, like many here today, continues to be a victim of ransomware incidents. Our National Health Service was affected by the Wannacry ransomware strain in 2017, from which the recovery cost $118 million. That money could have been spent on saving lives. This year, a critical supplier to London's hospitals was affected by a ransomware incident that postponed more than 10,000 health appointments and more than 1,700 medical procedures. That disruption is replicated across our critical sectors. It is why the United Kingdom considers ransomware one of our most significant cyberthreats to national security. To counter it, the United Kingdom is working to break the ransomware business model and discourage victims from paying the criminals. Alongside international partners, the United Kingdom has issued 36 sanctions against actors involved in these types of activities. However, we need a global response to this global threat.

First, we urge others to join the United Kingdom Government in not paying ransoms. In October, the United Kingdom and 49 other members of the International Counter Ransomware Initiative signed a public statement committing Governments not to pay ransoms.

Secondly, coordination will be our best defence. Recently, United Kingdom law enforcement led a coalition of global law enforcement agencies to disrupt the Lockbit ransomware group, the most prolific ransomware group of 2024.

Thirdly, we must increase resilience to these attacks by sharing information to illuminate the threats and build our collective understanding. We will continue to cooperate with international partners and industry to counter ransomware and dismantle the cybercriminal ecosystem.

I resume my functions as President of the Council.

I now give the floor to Mr. Lambrinidis.

Mr. Lambrinidis: I have the honour to speak on behalf of the European Union (EU) and its member States. The candidate countries North Macedonia, Montenegro, Serbia, Albania, Ukraine, the Republic of Moldova, Bosnia and Herzegovina and Georgia align themselves with this statement.

When hospitals, laboratories and emergency services are paralysed by ransomware, the impact extends beyond any single nation, placing patients' lives at risk, destabilizing healthcare systems and undermining trust in essential public services. Every 11 seconds a ransomware attack takes place, a rate expected to escalate to an attack every two seconds by 2031. The global nature of ransomware and its potential impact on international peace and security demand that we respond collectively and decisively to prevent future harm.

To prevent the threat, the European Union is taking strong action to protect critical infrastructure and essential services, including healthcare. We are boosting our defences, increasing our responses and strengthening our international partnerships to address the rising amount of ransomware. The EU's Network and Information Security Directive, adopted in December 2022, sets out cybersecurity risk management and incident reporting requirements for critical sectors across the EU and recognizes health as a "sector of high criticality". That ensures cybersecurity requirements for health facilities. The measures are intended to safeguard our healthcare, secure sensitive medical data and ensure that essential services remain operational despite cyberattacks. In other words, we recognize ransomware as a critical threat and reaffirm the urgency of the issue on the EU's political agenda.

In addition to prevention, we have also stepped up our responses to malicious cyberactivities, in particular ransomware attacks. In June, the EU imposed restrictive measures on individuals linked to ransomware campaigns. In addition, in February, the EU Cybercrime Centre, together with international partners, launched an operation to dismantle the LockBit ransomware group, one of the most prolific ransomware operators

globally. We are taking action using all instruments at our disposal against those who deliberately disrupt critical services. We also strongly call on all States, in line with the United Nations framework for responsible State behaviour, not to allow their territory to be used for such malign activities and respond to appropriate requests to mitigate such activities.

Finally, we will continue to strengthen partnerships to address ransomware threats through EU capacity-building initiatives such as supporting the development of national cybersecurity strategies and improving crisis management. The establishment of a permanent United Nations mechanism — a United Nations cyber programme of action — will allow us to advance our collective ability to counter threats against our societies and economies such as ransomware. The European Union stands ready to continue to work with the global community as well as the private sector to protect critical infrastructure, especially healthcare, from cyberthreats. Together, through a united and coordinated global approach, we can effectively combat the escalating threat of ransomware.

The meeting rose at 12.05 p.m.