

Tuesday, November 3, 2026

WELCOME ADDRESS BY HON. SAMUEL NARTEY GEORGE (MP), MINISTER FOR COMMUNICATION, DIGITAL TECHNOLOGY AND INNOVATIONS, AT THE REGIONAL SYMPOSIUM ON GOVERNING COMMERCIAL CYBER INTRUSION CAPABILITIES

LABADI BEACH HOTEL, ACCRA.

Your Excellency, Diarra Dimé-Labille, Ambassador of France to Ghana;
Mr Christian Rogg, British High Commissioner to Ghana;
Ms Sarah Osborn of the Foreign, Commonwealth and Development Office of the United Kingdom;
Mr Moses Faya, Founder and Policy Lead of Tech Policy Advisory, Nigeria;
Mr Abdul-Hakeem Ajijola, Chair of the African Union Cyber Security Expert Group;
Professor Nnenna Ifeanyi-Ajufo, Professor of Law and Technology at Leeds Beckett University and Vice-Chairperson of the African Union Cyber Security Expert Group;
Mr Alexandre Faidy, Policy Officer at the French Ministry for Europe and Foreign Affairs;
Distinguished representatives of governments, international organisations, law enforcement, industry, academia and civil society;

Ladies and gentlemen,

Good morning, and akwaaba to Ghana! Africa's warm heart and where God comes to rest!

It is my pleasure to welcome you to Accra. I thank the French Ministry for Europe and Foreign Affairs, the Government of the United Kingdom, the European Union, Expertise France and Ghana's Cyber Security Authority. You have brought us together for a conversation that matters. Ghana is grateful.

Ladies and gentlemen, let me begin with a simple picture.

Think of the phone in your pocket. It holds your messages. Your photographs. Your mobile money. Your location. For millions of our citizens, that phone is their bank, their office and their family album.

Now imagine a tool that can enter that phone without your knowledge. It can read every message. It can switch on the microphone. It can follow every step you take. And you would never know.

Such tools exist. They are built by private companies. They are sold on a commercial market. That is what we mean by commercial cyber intrusion capabilities.

Some governments acquire these tools to fight terrorism and serious crime. That purpose can be legitimate. But without clear limits, the same tools can be turned on journalists, activists, political actors, business leaders and ordinary citizens. They erode privacy. They weaken public trust. They can damage the very institutions they were meant to protect.

So the question before us is not only what these tools can do. The real question is this: who is accountable when they are misused?

This is why the Pall Mall Process matters. Launched by the United Kingdom and France, it brings governments, industry and civil society to one table. Its purpose is clear. To build a shared understanding of responsible behaviour. And to act against the spread and irresponsible use of these capabilities.

Distinguished guests, I wish to draw a clear distinction this morning. It sits at the heart of this symposium.

Every State carries two responsibilities in cyberspace.

The first is the duty of restraint. When the State uses cyber capabilities to protect the nation and its people, it must act within the law. It must act only when necessary. It must act in proportion to the threat. And it must answer to independent oversight. These powers exist to protect citizens. They must never be turned against them.

The second is the duty of protection. The State must have the capacity to defend its citizens from those who mean them harm. Cybercriminals. Fraudsters. Hostile actors. Unscrupulous vendors who will sell intrusion tools to anyone who can pay. A State that cannot detect, investigate and stop these threats leaves its people exposed.

These two duties are not in conflict. They depend on each other.

A State that restrains itself but cannot protect fails its citizens. A State that protects but does not restrain itself betrays its citizens.

Our task is to hold both. That is why Ghana rejects the false choice between security and human rights. Sustainable digital security requires both.

Ladies and gentlemen, let me set out how Ghana is organised to meet both duties, and the role of my Ministry.

The Ministry of Communication, Digital Technology and Innovations sets national cybersecurity policy. We shape the law. We set the direction. We coordinate across government. And we represent Ghana in regional and international processes such as this one.

Our foundation is the Cybersecurity Act, 2020 (Act 1038). That Act established the Cyber Security Authority as Ghana’s cybersecurity regulator, under my Ministry's oversight. The Authority protects our critical information infrastructure. It leads our national response to cyber incidents. It also licenses cybersecurity service providers, accredits cybersecurity establishments, and certifies cybersecurity professionals.

That last point matters for today. In Ghana, cybersecurity service providers must be licensed. This market is not ungoverned. Licensing gives us a practical lever to shape conduct in the very commercial space this symposium is examining.

Our framework also rests on the Data Protection Act, 2012 (Act 843), administered by the Data Protection Commission. In Ghana, privacy is not an afterthought. It is a pillar.

The division of responsibility is clear. The Ministry makes policy. The regulators enforce. Parliament legislates and scrutinises. The courts safeguard rights. Each has a role. None stands alone.

Technology moves fast. Our laws must keep pace. My Ministry will keep our legal and policy framework under review, so that it responds to tools like those under discussion today. The outcomes of this symposium will inform that work.

To turn principle into practice, I propose that our deliberations focus on three stages of accountability.

First, accountability before acquisition. Before any State acquires these tools, it must answer hard questions. Is there a clear legal basis? Who authorises the purchase? Has the vendor been properly examined? What are the human rights risks?

Second, accountability during use. Every use must be authorised, recorded and reviewed. Oversight must be independent. It must be real, not symbolic.

Third, accountability after harm. When things go wrong, victims must have a remedy. Misuse must be investigated. Those responsible, whether in government or in industry, must answer for it.

These three stages give the principles of the Pall Mall Process practical shape. They can be measured. They can be applied at home and across borders.

Distinguished guests, Africa must not be a passive observer in shaping the future of digital security. We will not simply receive rules written elsewhere. We must help to write them.

Our countries face real threats. We must protect our critical infrastructure. Our power systems. Our banks. Our mobile money platforms. Our hospitals. We must investigate

serious crime and safeguard national security. Equally, our citizens deserve protection from unlawful and disproportionate intrusion.

We have foundations on which to build. The African Union Convention on Cyber Security and Personal Data Protection is now in force. Our responsibility is to turn that commitment into effective national laws, stronger institutions and meaningful regional cooperation.

As Chair of the African Union Specialised Technical Committee on Communication and ICT, I will ensure that the outcomes of this symposium reach our continental partners.

Ladies and gentlemen, allow me to speak to every technology user. To the seasoned engineer in this room. And to the young trader in Tamale who opened her first mobile money account last month.

Cybersecurity is not only for experts. It belongs to all of us.

To the experienced, I ask for leadership. Build systems that are secure by design. Share threat information. Hold your industry to the highest standards.

To those who are new to technology, my message is simple. Your phone is valuable. Protect it. Keep it updated. Use strong passwords. Be careful with links and attachments from people you do not know. And if something feels wrong, report it. Call or text 292 to reach the Cyber Security Authority.

In return, the Government's promise is equally simple. We will protect you from those who would harm you online. And we will ensure that the powers we hold to protect you are never used to wrong you.

This conversation connects directly to Ghana's wider digital ambition. We are building a digital economy that is secure, trusted and inclusive.

Our principle is clear. Ghana does not simply want to adopt emerging technologies. We want to shape them, govern them and deploy them responsibly.

Innovation without accountability creates new vulnerabilities. Responsible governance builds trust. And trust is the currency of the digital economy.

Ladies and gentlemen, I urge this symposium to move beyond broad declarations. Give us practical recommendations. Recommendations that governments can legislate. That technology providers can implement. That oversight institutions can enforce.

Ghana is honoured to host this conversation. We will contribute actively to the Pall Mall Process. We will work with our partners to build a framework that is globally relevant, rooted in African realities, and capable of delivering results.

On this note, it is my pleasure to declare the Regional Symposium on Governing Commercial Cyber Intrusion Capabilities officially open.

Obaake! I wish you fruitful deliberations and a successful symposium.

Thank you.