PRESS RELEASE

Global World Council publishes Cyber Strategy for the "resilience of the community"

6th December 2030

Thought Leader for Cyber Affairs, Arma Intence (pictured below), representing the Global World Council today (6th December 2030) announced the publication of the Council's Resilience of the Community Cyber Strategy.

Arma Intence, Thought Leader for Cyber Affairs, Global World Council

Anchored in the accessibility for the public and private sectors, the Strategy sets out security measures in the digital domain to protect ourselves against cyber threats, promote the desired supply chain resilience and safeguard the continuity of digital transformation, the continuity of technology and the continuity of the Internet.

The Strategy announces:

- Industrial programs to enhance the cyber security of the internet, including through the development of a secure by design capability to develop cyber-secure products and services,
- Internet standards and technical strategies to support citizens through comprehensive victim response, and be effective in peace time, and
- Constantly evolving international collaboration with the private sector.

In a global first, the Council's Cyber Strategy also announces the introduction of a cyber situation centre.

Launching the Strategy in Geneva, Thought Leader Intence commented:

> "Strength of cyber security is a common policy. Resilience of the community exists to support the community and society: we need to be confident in the digital security of the Internet.
>
> "Governments will require expertise: it will include many participants to achieve cyber security, prosperity and stability".

ENDS

UNDER EMBARGO

GLOBAL WORLD COUNCIL

Resilience of the Community Cyber Strategy

December 2030

Executive Summary

The strategy is to include the responsible authorities and academia and information systems and services that are addressing the research community and coordination of the community and security measures against cyber and information security in the digital domain names, and promoting information security and control systems and services and the community and security measures and all the continuity of the technology to comply with the internet. This sets out their international cooperation and information security in the digital domain and accessibility for the public and private sectors and the continuity of communication and international law in cyberspace and security measures to protect ourselves and the continuity of the strategy.

Key is ensuring the security of the cyber security architecture of the community and security and prosperity and security measures to protect ourselves against cyber threats, and the private sector and the protection and communication and expertise and deterrence and the security of the strategy. The Commission will continue to achieve this objectives and the community and support they need to be able to develop internet security measures that are increasingly secure and resilient for the nation.

In addition, the government will also strengthen the continuity of digital transformation and the competitiveness of the threat situation report to the protection of a comprehensive verification processes that are considerable, and that the informal level and strength of the cyber security is a common policy and resilience of the community exists to support the community and society. The government will also be able to manage the ability to advance the security of the security authorities and infrastructure in a common use of the threat situation report to the protection of a comprehensive victim response.

Objectives

The Government will examine attainment of the objective based on the private sector organisations that are well-placed to the detection of cyber-security incidents, in consultation with the Secretary of Homeland Security acting through the Director of NIST, and shall also be able to address the role of private industry, industrial programs to enhance the cyber security of the internet, the private sector and expertise that operate supply chains.

They will be able to encourage internet standards and allow the security of the police and international law and the approach to cyber threats consolidated to the development of a secure by design capability.

This will be addressed as an integral part of a protection and competent agencies will be within advanced cyber security and intelligence services by the form of the technical strategies to enable them to support citizens and be effective in peacetime.

The Government will invest £Xmillion through the successful digital resilience to international partners to increase the capabilities and advisory and quantitative operations, stimulating critical infrastructure services and international partners to protect themselves against attacks.
The Government will derive security measures to protect themselves and the development of devices that can be exploited at the same time, responsible for the continuity of the internet with the National Cyber Security Centre, providing a strong competitiveness with the public and private sectors and the constantly evolving international cooperation.

The NCSC provides a more complex and consumer protection responsible for the development of the public and private sectors and the community and security of the cyber security advice and the security authorities with the aim of existing assurance services that are developing cyber-secure

UNDER EMBARGO

products and services. At the same time, the strategic objectives and the provision of the cyber security and control systems and infrastructure is a standard, and other advanced information and control systems and attacks can be addressed in the field of cyber security and communications security and society as a whole.

What is our current position?

The government and international partners are to continue their respective competence and the security authorities and communications networks for the security authorities, to address international cooperation. It is a common risk management and international collaboration with the private sector including providers of the security of the international community and security standards, the role of the COVID-19 pandemic, and international cooperation on the board for government that in the EU and its Member States, committed to NATO's protection and the police and anti-terror services.

The UK is a platform and is to be established as a tool in the field of cyber security efforts required to advance the activities on sovereignty in cyber security and society to protect ourselves against cyberattacks and protecting our cybersecurity policy. This means that we are to be able to meet the definition of the law enforcement authorities and are confident in the digital security of the Internet and relevant stakeholders.

Measuring success

- ensuring provisions for the community will be provided
- assurance-body activity for businesses are accessible
- professionals recognised in compliance with the government
- EU's vulnerabilities and remedy
- cyber security units put into intercepted lines
- platforms and businesses and the requirements issued to meet key AI functions
- The cyber situation centre will be introduced
- increasing international cooperation and coordination with the Director of NCSC, in consultation with Cyber Security Strategy
- Encryption in the National Crisis Centre

In addition, the government will require expertise to enhance the ability to detect attacks that can be advanced to the definition of computer systems and the provision of personal data.

The mission of cyberspace and the country has responsible authorities and academia to make use of the sector and the protection of the community, and to respond to consumers by the framework of specific advisory provision of digital services that are complementary, and promote the desired supply chain resilience.

This will include many participants in the sector of cyber security professionals to achieve cyber security and prosperity and stability with strong communication and compliance.

This is an AI-generated document and does not represent the views of NCC Group or its employees.

UNDER EMBARGO