Countering DPRK Cyber Threats:
An Interactive Virtual Training for Financial Institutions in Nepal

18 March – 19 March
9:30 am – 12:30 pm GMT +5:45 (Local NPT Time)

This virtual training will show participants how to identify and prevent state-sponsored cyber-attacks, including the Democratic People's Republic of Korea (DPRK).

This **2-day virtual training** is tailored for managers, network administrators, and cybersecurity personnel from financial institutions and the central bank in **Nepal**. According to the United Nations, North Korea repeatedly targets the region with cyber-attacks to gain access to currency and launder money in violation of international sanctions.

An expert team of cybersecurity specialists from **Internet 2.0** will lead interactive sessions on DPRK cyber thefts, techniques to manage incidents, and how to strengthen your institution's cybersecurity against advanced persistent threats. Participants will develop an enhanced threat awareness of DPRK cyber activities that negatively impact your financial institution and country. This training will prepare you to identify malware, SWIFT attacks, and other schemes to improve your ability to conduct intelligence assessments, practice threat hunting, and implement cybersecurity best practices.

Registration and Fees:
This virtual training is **offered free of charge**, but the interactive exercises mean that space is limited.

To register please click here:
https://cvent.me/RbRwXl

Registration ends
15 March 2021

The training will be conducted over Zoom and will require access to a computer or the Zoom mobile application. You can download the Zoom application for free or attend the meetings through your browser.

For more information, please see the registration website or contact Zach Goble (zgoble@crdfglobal.org)

Why Attend?
- Learn about the latest case studies on DPRK cyberattacks in the region and around the world.
- Strengthen understanding of DPRK cyber threats and activities, common system vulnerabilities, and institutional cybersecurity best practices.
- Learn about threat intelligence, threat hunting and incident response.
- Engage in scenarios around managing incidents.
- Develop an understanding of cyber security and how it relates to financial services and the SWIFT platform.

Internet 2.0

CRDFGLOBAL

The Internet 2.0 and CRDF Global Team

Internet 2.0 is an Australian technology start-up. Founded by Robert Potter and David Robinson, these two experienced cyber security executives have concluded that cyber security, as it stands, leaves countries, companies, and users too vulnerable, and coverage too expensive. Internet 2.0 exists to change the basic structure of the internet. Cyber security should not just be available to large corporate clients, but to all citizens. By flipping the paradigm on its head, Internet 2.0, develops capabilities which harden core networks by leveraging their own bespoke security hardware. Internet 2.0 is regularly engaged as a trusted partner by Governments in the Asia-Pacific region.

Robert Potter currently is the Chief Executive Officer of Internet 2.0, a cyber security startup which works to fortify networks and online communications. Prior to this, he was the Head of Cyber Operations at BAE Systems Applied Intelligence. An experienced cybersecurity executive and incident response lead who has held senior advisor roles in Cyber Security within the Australian Shadow Cabinet and Government. A former advisor to the Board of the New Payments Platform, a real time SWIFT based payment system deployed by the major banks within Australia. He regularly consults to financial institutions, human rights organizations, and governments within Asia on securing their systems from cyber-attacks against North Korea.

Patrick Hamilton has been involved in the computer field for over two decades, including the start-up of the world's largest network of over 360,000 workstations. He has also worked with making networks operational and secure in remote locations requiring satellite connectivity, including marine, airborne and ground based systems. Recently, he has provided computer technical expertise to the Papua New Guinea National Cyber Security Centre (NCSC) and The Washington Post news agency. He is currently a cyber security Partner with Internet 2.0. Courses developed by Patrick have been accredited by both the United Kingdom's GCHQ and United States' ANSI.

David Robinson is an experience intelligence and cyber security specialist. He has worked extensively in open source intelligence in defense and the private sector. David has led critical infrastructure uplifts within the Asia-Pacific including being the coordinator of the engagement to uplift APEC's cyber security in 2018. He recently responded to a DPRK cyber attack within Australia

Adam O'Donnell is a qualified and experienced trainer with a background in critical infrastructure. Across a diverse career Adam has been responsible for responding to a number of the region's largest cyber attacks. Including leading the response to the Australian Bureau of Meteorology and other major providers. For the past ten years he has been a leader in the space. Prior to his career in cyber security management Adam was a special operations team leader in both the British SAS and the Australian Commandos.

CRDF Global is an independent nonprofit organization that provides international training and capacity building to advance international peace and security. In the past 25 years, our work has expanded to address ever-changing global concerns, but our commitment to ensuring the success of our partners remains the same. We are a leading provider of flexible logistical support, program design and management, and strategic capacity building programs in the areas of higher education, CBRNE security and nonproliferation, border security, cybersecurity, and more. CRDF Global's diverse staff and networks of local community and government stakeholders deliver tailored programs that meet specific regional needs in over 100 countries across the globe.