25

2120

Registrar Office Diary 1423 21/05/25 MNSUAM

No.E&A (Agri)6-334/2025
GOVERNMENT OF THE PUNJAB
AGRICULTURE DEPARTMENT

Dated Lahore, the 12th May, 2025

To

1. The Managing Director, Punjab Seed Corporation, Lahore.
2. The Director General Agriculture (Extension), Punjab, Lahore.
3. The Director General Agriculture (FT & AR), Punjab, Lahore.
4. The Director General Agriculture (Field) Punjab, Lahore.
5. The Director General Agriculture (WM), Punjab, Lahore.
6. The Director General, PW & QC of Pesticides, Punjab, Lahore.
7. The Director General, Soil Survey of Punjab, Multan Road, Lahore.
8. The Director General Agricultural Information, Punjab, Lahore.
9. The Director General, Crop Reporting Service, Punjab, Lahore.
10. The Director Floriculture (T&R), Punjab, Lahore.
11. The Chief Executive, Punjab Agricultural Research Board, Lahore.
12. The Chief Scientist Agriculture (Research), AARI, Faisalabad.
13. The Chief, P&E Cell, Agriculture Department, Lahore.
14. The Chief Coordinator, RAEDC, Vehari.
15. The Chief Technical Advisor, Agriculture Delivery Unit (ADU), Lahore.
16. The Secretary Agriculture Commission, Lahore.
17. The Registrar, University of Agriculture, Faisalabad.
18. The Registrar, Arid University of Agriculture, Rawalpindi.
19. The Registrar, Muhammad Nawaz Sharif University of Agriculture, Multan.

Subject: - **CYBERSECURITY ADVISORY ON STRENGTHENING CYBER VIGILANCE AND RESILIENCE AMID RISING GEOPOLITICAL TENSIONS**

Please find enclosed herewith a copy of a letter No.SO(FG-II)6-3/2024 dated 03.05.2025 alongwith its enclosure, received from Section Officer (FG-II), S&GAD, on the subject cited above, for information and compliance.

SECTION OFFICER (GENERAL)
Ph. No.99200518

n/a pl.

21/05/25

Director IT/ DR(I+R)

Ms. Rawda
Please upload on website

NO.SO(FG-II)6-3/2024
GOVERNMENT OF THE PUNJAB
SERVICES & GENERAL ADMINISTRATION DEPARTMENT
(IMPLEMENTATION & COORDINATION WING

Dated: Lahore the 3rd May, 2025

PATO SECY AGRI
Diary No. 2841
Date 8/5/2025

To

1. **The Senior Member,** Board of Revenue, Punjab.
2. **The Chairman,** P&D, Board, Punjab
3. **The Additional Chief Secretary,** Punjab.
4. **The All Administrative Secretaries,** Govt. of the Punjab.
5. All **the Divisional Commissioners,** Punjab.
6. The **Chairman,** PITB, Lahore.

SS Agri	
AS (A)	✓
AS (F)	
AS (TF)	
Chief P&EC	
PO	
PS	

Subject: **CYBERSECURITY ADVISORY ON STRENGTHENING CYBER VIGILANCE AND RESILIENCE AMID RISING GEOPOLITICAL TENSIONS**

Kindly refer to the subject cited above and find enclosed herewith a copy of letter No. 1-1/2024/DGRC (nCERT)/198 dated 27.04.2025 alongwith its enclosures received from Director General, National CERT, National Cyber Emergency Response Team, Government of Pakistan, Islamabad for information and necessary action.

(ZAHEER AHMAD BABAR)
SECTION OFFICER (FG-II)

C.C:

i. Director General, National CERT, National Cyber Emergency Response Team, Government of Pakistan, Pak Secretariat, L Block, Islamabad w.r.t above mentioned letter.
ii. PSO to Chief Secretary, Punjab.
iii. PS to Secretary (I&C), S&GAD.

E & A Section
Diary No. 3560
Date 12-5-25
Govt. of the Punjab
Agri. Deptt.

PPU
9/5/25

SO(FG)

Deputy Secretary (Admn-I)
Government of the Punjab
Agriculture Department

Deputy Secy. (A-I)
Dairy No. 3610

National Cyber Emergency Response Team

Government of Pakistan

PKCERT

F.No.1-1/2025/DG (nCERT)/198

Dated, the 27 April, 2025.

Subject: **Cybersecurity Advisory on Strengthening Cyber Vigilance and Resilience Amid Rising Geopolitical Tensions**

In light of the rising geopolitical and regional tensions, and the heightened threat landscape impacting national cybersecurity, the attached Advisory titled "*Cyber Vigilance Required in the Wake of Rising Geopolitical/Regional Unrest*" (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).

2. The Advisory outlines the potential cyber threats, identified tactics and vectors, and prescribes critical immediate and strategic cybersecurity measures required to protect national interests, critical infrastructures, and public trust.

3. It is requested that the attached Advisory may kindly be disseminated to all relevant departments and organizations under your administrative control, and necessary action may be taken accordingly to ensure heightened vigilance and readiness.

Annexure: NCA-18.042725 – NCERT Advisory – Cyber Vigilance Required in the Wake of Rising Geopolitical/ Regional Unrest

Dr. Haider Abbas, TI
Director General
National CERT
Ph: 051-9203422

All Secretaries of Ministries/ Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

NCA-18.042725 – NCERT Advisory – Cyber Vigilance Required in the Wake of Rising Geopolitical/ Regional Unrest

Introduction

In light of the escalating geopolitical tensions, particularly across Central Asia and more specifically the South Asian region, the National Cyber Emergency Response Team (National CERT) issues this high-priority advisory urging heightened vigilance and immediate cybersecurity precautions. The volatile environment in these regions could be exploited by adversaries, including state-sponsored threat actors, hacktivists, and opportunistic cybercriminal groups. These actors may attempt to target sensitive sectors such as government agencies, critical infrastructure, defense, media, finance, and individual assets within Pakistan.

Observed tactics may include spear-phishing, advanced malware deployment, disinformation campaigns, deepfakes, supply chain compromise, and critical service disruption (DDoS). Attackers could also employ Advanced Persistent Threat (APT) techniques to gain prolonged, stealthy access to sensitive networks, making them harder to detect and mitigate.

Timely action is crucial to prevent potential espionage, data theft, operational disruption, and public misinformation, which could undermine national security, economic stability, and public trust.

Impact

Successful exploitation can lead to:

1. **Data Breach and Espionage** – Unauthorized access to sensitive government, military, and personal data, with potential for espionage or intelligence gathering, severely affecting national security.
2. **Critical Infrastructure Disruption** – Cyberattacks targeting energy, telecommunications, transportation, and other vital public services, potentially leading to widespread disruptions and loss of services.
3. **Disinformation and Psychological Operations (PSYOPS)** – Misinformation campaigns designed to destabilize public trust, disrupt political stability, and incite unrest through false narratives, including deepfake videos and fabricated social media content.
4. **Financial Theft and Ransomware** – Compromise of financial institutions or critical banking systems, potentially leading to data breaches, ransomware attacks, and significant financial losses.

5. **Supply Chain Compromise** – Attackers may infiltrate trusted vendors or service providers to gain unauthorized access to critical systems. Malicious code insertion into software updates can also disrupt entire organizations.
6. **Account Takeover (ATO)** – Hijacking official and personal accounts, including government portals, media outlets, and banking accounts, to further disrupt operations, steal data, or spread false information.

Threat Details

Attack Vectors

The evolving threat landscape includes various sophisticated attack vectors, including, but not limited to:

- **Spear-Phishing Emails and Messages**: Highly personalized and context-aware lures designed to target government and military personnel, often using social engineering tactics to induce trust.
- **Malicious Mobile Apps**: Fake apps, often masquerading as legitimate news, finance, or social media platforms, are being used to embed spyware or deploy keyloggers on the victim's device. App permissions may also be exploited to access sensitive data without user knowledge.
- **Fake News Websites and Social Media Pages**: These fraudulent platforms are designed to spread disinformation, disrupt peace, and sow chaos in social and political spheres. Fake accounts and bots may amplify these campaigns, creating a false narrative that is hard to detect.
- **DDoS Attacks**: Distributed Denial of Service (DDoS) attacks aimed at overloading critical services such as government portals, financial institutions, and emergency response networks, leading to outages or loss of public trust in essential services.
- **Deepfakes and Synthetic Media**: AI-generated deepfakes—including audio, video, and images—used to impersonate high-profile officials or public figures, potentially leading to reputational damage or triggering geopolitical tension through false statements.
- **Credential Stuffing and Brute Force**: Attackers exploiting weak passwords, especially those reused across multiple platforms, to gain unauthorized access to both official and personal accounts. Automated attacks against user login credentials are increasingly effective if strong password policies are not in place.

Threat Actors

The threat actors likely to exploit this environment include:

- **State-Sponsored APT Groups**: Highly skilled and well-resourced groups with political motives, focusing on espionage, surveillance, and the disruption of critical national assets. These actors often leverage zero-day vulnerabilities and employ advanced tactics, techniques, and procedures (TTPs) to avoid detection.
- **Cybercriminal Gangs**: Opportunistic actors targeting individuals and institutions for financial gain, using ransomware, phishing, and fraud tactics.
- **Hacktivists**: Groups with political or ideological motivations aiming to disrupt public services, government operations, or political stability through denial-of-service attacks, leaked data, or disinformation.

Affected Systems

The systems at the greatest risk during these times include:

- **Government Agencies**: Including ministries, defense establishments, and public service departments responsible for national security and governance.
- **Critical Service Providers**: Including telecommunications, energy, transportation, and water—all vital for public welfare. These services are prime targets for disruption or data theft.
- **Financial Institutions and Banking Infrastructure**: These systems are particularly vulnerable to ransomware, account takeovers, and theft.
- **Media Outlets, Public Figures, and Journalists**: Targeted for disinformation campaigns and social media manipulation to alter public perception.
- **General Public**: Individuals using mobile, social, and cloud services are at risk of being exposed to phishing, malware, and fake news campaigns.

Recommendations & Action Items

1. Immediate Mitigation Measures

a. Strengthen Authentication

- Enforce mandatory use of Passkeys (FIDO2/WebAuthn) or multi-factor authentication (MFA) across all critical accounts and services.

- Disable SMS-only authentication, as it can be easily bypassed. Prefer hardware-backed security keys for high-risk accounts.

b. **Patch and Update Systems**

- Immediately patch all critical software, including Operating Systems (OS), VPNs, firewalls, and email servers to mitigate known vulnerabilities.
- Update antivirus/EDR solutions with latest threat signatures and make sure systems are continuously monitored for new threats.

c. **Secure Communications**

- Use end-to-end encrypted communication platforms for sensitive communications.
- Avoid sharing classified or sensitive information via personal messaging apps or unsecured channels.

d. **Secure Endpoints**

- Implement application whitelisting to block unapproved applications from running on enterprise devices.
- Deploy mobile threat defense (MTD) solutions on smartphones to monitor and block malicious mobile activity.

2. Proactive Threat Detection

a. **Monitor Network Traffic**

- Enable deep packet inspection (DPI) on critical network traffic to detect suspicious activity, including command-and-control traffic.
- Implement real-time traffic analysis to identify and isolate anomalous network traffic patterns that might indicate an active attack.

b. **Enhanced Logging and SIEM Monitoring**

- Ensure all access logs are comprehensive and actively monitored.
- Set up alerts for suspicious login attempts, especially from foreign geographies, to quickly identify possible intrusion attempts.

3. Incident Response Preparedness

- Review and update incident response plans to reflect the evolving threat landscape and ensure rapid response during a crisis.

- Conduct tabletop exercises simulating cyber incidents during geopolitical crises to ensure all stakeholders are prepared.
- Maintain offline, air-gapped backups of critical data to ensure recovery even in the event of a cyberattack.
- Report any incidents to National CERT for immediate assistance:
  a. **Incident Reporting Form**: [https://pkcert.gov.pk/report-incident/]
  b. **Email**: cert@pkcert.gov.pk

4. Cyber Hygiene and User Awareness

- Launch cybersecurity awareness programs across all levels of personnel to foster a security-first mindset.
- Educate users to:
  - Verify links and attachments before clicking, even if they appear to come from trusted sources.
  - Avoid downloading unverified mobile applications that could compromise device security.
  - Report suspicious emails, calls, or texts immediately.
- Provide training on how to identify fake news and instruct personnel on how to report disinformation campaigns.

Strategic Protective Measures

- Implement Zero Trust Architecture (ZTA) to prevent unauthorized access within critical environments.
- Restrict foreign IP ranges from accessing sensitive government systems, minimizing external attack surface.
- Conduct thorough audits of third-party vendors to ensure cybersecurity compliance across the supply chain.
- Enhance encryption standards for data at rest and in transit, ensuring data security across all communication channels.

Disaster Recovery & Business Continuity

- Ensure redundant communication channels in case of internet or network disruptions.

- Maintain emergency response coordination plans between government agencies to streamline recovery during a cyber crisis.
- Periodically test critical infrastructure backup systems to verify their ability to restore operations in the event of a cyberattack.

Patching & Updates Focus

Risk	Recommendation
Outdated VPNs/Firewalls	Apply latest firmware and patching immediately.
Unpatched Operating Systems	Implement automatic critical patching across all systems.
Mobile Device Vulnerabilities	Regularly update apps and OS; restrict unauthorized app installations.
Email Servers	Harden against spoofing, phishing, and spam to prevent social engineering attacks.

Call to Action

The National CERT strongly advises:

- All government departments and critical organizations to immediately implement heightened cybersecurity defenses and carry out a thorough security audit of their infrastructures.
- Individuals should practice good cyber hygiene, avoid engaging with misinformation, and use secure communication tools.
- IT teams must proactively hunt for potential threats, secure infrastructures, and educate end-users to foster a secure environment.