Tabletop exercise on cyber crisis with Malaysia's security sector

Workshop report

Table of content

Glossary of abbreviations

Abbreviation	Definition
AI	Artificial Intelligence
ASEAN	Association of Southeast Asian Nations
SITREP	Situation Report
TTX	Tabletop Exercise
UN	United Nations

Foreword

While Vegetius' famous adage is vis pacem, para bellum – if you want peace, prepare for war – may still hold true for conventional warfare, a strategic recalibration is warranted in the cyber realm. This is where warfare descends like a frog in a cauldron – steeping slowly from operations below the threshold of force such as disinformation and influence operations, escalating to activities that incapacitate critical infrastructure, crippling government services and deep freezing the economy. This is the reality of Stuxnet and Estonia, which at scale, could impair a nation while recovery could span weeks or months.

Malaysia is on track to be an AI nation. With 98% of Malaysian households using the Internet and having access to smartphones, Malaysia's digital canvas will be sophisticated, complex and ubiquitous. Federal and state governments are adopting AI in services, whether for chatbots, demographic data analytics or to reduce workloads in courts. Increasingly this enlarging intertwined digital and physical terrain would serve as a tantalizing target for malicious parties.

Yet, depictions of incapacitating cyberattacks can be more exaggerated than real. Science fiction captures the imagination with rogue AI in the form of killer robots or omniscient intelligent computer systems whose access rival supreme beings, even God. Such depictions aren't anchored on reality where discrepancies in data infrastructure, limiting regulations, levels of AI adoption and market competition may mean that in the civilian sphere, no AI rules supreme. However, the Russia-Ukraine war illustrated how disinformation and misinformation architectures could be harnessed for a war of perception. Soldiers could lose the will to fight as a nation's Jus ad Bellum is brought into question. Furthermore, a cyber incident in a single facility could induce unintended consequences on nearby infrastructure, thus disrupting both civilian and military services.

Such incidences could take advantage of ambiguity in thresholds of response. International law, particularly the Charter of the United Nations, is applicable in cyberspace, according to the report by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2013. However, yet to be formulated are rules governing the impact of cyber incidences on sovereignty. Further, norms of accepted responses differ, where certain states legitimize the use of military response to a cyber incident above a certain threshold.

While constructing the appropriate retaliatory measures to deter future attacks is a major challenge, there is the added pressure to publicly attribute malicious actors. With a growing trend of joint public attribution, developing countries such as Malaysia, would be expected to construct guidelines for norms of response and public attribution, especially to demonstrate cyber power in the digital age.

In the midst of cyber incidences, nations can be myopic about recovery. It has only been 15 years since Malaysia surpassed 50% of broadband subscribers, 17 since the first National Cyber Security Policy was introduced and eight since inaugurating the National Cyber Security Agency. Meanwhile, digital has become the portfolio of every ministry where in one way or another, an agency uses or governs cyber, be it for their own systems or the public. However, at a time of crisis, would responsibilities be known or could bureaucracy and uncertainty stifle solutions?

It is to answer these questions that the Institute proposed a tabletop exercise on cyber with the security sector. As was the case of US responses to the Japanese in World War II, wargaming and tabletop exercises could test responses in a crisis situation, while shoring policies that strengthen resilience. During the Cuban Missile Crisis, simulations projected potential reactions by adversaries and tackled misperceptions that would otherwise escalate conflicts. Governments, therefore, saw it in their interest to pursue a path of greatest stability, particularly to prevent intensified situations getting out of hand. In cyberspace, where malicious actors and defenders could be shrouded in similar streams of bits and code, tabulating responses is essential to keep conflicts and crises in check.

The exercise simulates a cyber crisis with the purpose of testing interagency response. The program would not be possible without the support of the US Embassy in Kuala Lumpur and Professor Greg Austin from the Social Cyber Academy, Dr Jay Jeong of TNK, Professor Atif Ahmad from the Melbourne Security Associates and Ts Mohamed Kheirulnaim Mohamed Danial from Malaysia's National Cyber Security Agency. In as much as the exercise held on September 22 yielded valuable insights and lessons, such programs would be of considerable value towards improving Malaysia's response to crisis for the future.

Datuk Prof Dr Mohd Faiz Abdullah
Chairman
ISIS Malaysia

Opening remarks

The tabletop exercise organized by ISIS Malaysia and the US Embassy carries the theme "Untangling the Algorithm: Cross-Border Collaboration and Security Issues with Artificial Intelligence." The theme speaks to the complexity of the challenges before us and to the urgency with which they must be confronted.

Artificial Intelligence is no longer confined to the academic laboratory or the realm of science fiction. It has become embedded in every artery of national life, shaping our communications, our critical infrastructure, and increasingly, our instruments of defense. We are gathered here not simply as academics, policymakers, or practitioners, but as guardians of national resilience. The world is transforming at a velocity unprecedented in human history and at the heart of this transformation lies Artificial Intelligence. While AI promises prosperity, innovation, and efficiency, it also introduces risks that are unlike anything we have encountered before—risks that cut across safety, security and defense.

This exercise is not a routine seminar. It is a strategic rehearsal. It is an opportunity to prepare for crises that are no longer hypothetical, but inevitable, that could happen, spark anytime and anywhere.

Part I – The Promise and Peril of AI

Artificial Intelligence has already moved far beyond research papers and prototypes. It is today a decisive factor in civilian life and security affairs. In defense and security, AI offers extraordinary opportunities. It allows us to deploy autonomous drones and unmanned vessels that extend surveillance across vast oceans and contested airspaces. It enables predictive analytics to anticipate smuggling routes, terrorism financing, and cyber intrusions. It equips commanders with decision-support systems that capable of processing vast amounts of data within seconds. It actually generates required information from raw data faster, guiding instantly and more accurate operational responses. Besides that, it strengthens logistics and supply chain resilience, ensuring that forces in the field remain supplied and combat ready.

Nations that harness AI are not just gaining economic advantages, but they are securing strategic dominance. Around the world, advanced militaries are integrating AI into war-gaming, satellite reconnaissance, missile guidance and electronic warfare. It is not an exaggeration to say that the race for AI supremacy is becoming as consequential as the nuclear race of the last century.

Up to date, AI is not inherently ethical enough. Algorithms do not share human values, and they are possible to be manipulated or misused. We must reckon with the possibility of deepfakes and synthetic media that distort truth, eroding public trust in leaders, institutions, and even the armed

forces. We must anticipate AI-driven cyberattacks where they are highly possible and capable of paralyzing power grids, disabling military communications and even disrupting command-and-control systems. We must guard against autonomous weapons, misinterpreting signals and escalating conflicts without human oversight. And we must be prepared for vulnerabilities in border control, financial systems, or logistics chains that could be exploited to destabilize nations from within.

The critical question before us is not whether AI will create crises. The real question is when those crises will strike, and how well we prepared to respond and react.

Part II – AI and National Security

For Malaysia, and indeed for our region, AI represents a double-edged sword. On one side, it strengthens defense. AI-enabled drones now extend surveillance across our vast maritime zones, giving us unprecedented awareness of our surrounding waters, in other words, a better situational awareness. Predictive tools can help to detect illicit trade, human trafficking, and cyber threats targeting our systems. Decision-support platforms powered by AI can vastly improve our national response to natural disasters, pandemics, and humanitarian crises, ensuring lives are saved and resources optimized. An advanced AI system is able to assist in decision making process at strategic level where it considers all possible outcome and impact based on previous history and behavior patterns.

But on the other side, the dark shadows, AI introduces vulnerabilities that are strategic in nature. Hostile powers could weaponize algorithms to cripple communication networks or financial markets. Malicious actors could deploy deepfakes to spread disinformation about our leaders, sway public trust and sowing discord in our democracy. A compromised autonomous system, whether a drone, vehicle, or naval platform, could escalate a standoff into conflict without a shot being deliberately fired.

These are not abstract dangers. They are already with us. We have witnessed the AI based ransomware attack on 7th May 2021 in Colonial Pipeline of United States which paralyzed energy supplies. We have seen AI-generated disinformation campaigns influencing elections across the world. We have watched drone swarms in the Ukraine conflict demonstrate how low-cost, AI-enabled systems can overwhelm conventional defenses.

For Malaysia, a nation that depends on digital infrastructure, maritime security, and regional trade, the line between civilian disruption and military threat is increasingly blurred. National security in the age of AI is inseparable from societal resilience.

Part III – The Need for Cross-Border Collaboration

The most sobering reality is that AI-driven crises will not respect sovereignty. A virus unleashed in one country's servers can cascade across borders within hours. A manipulated financial algorithm in one market can send shockwaves through the global economy. A disinformation

campaign orchestrated abroad can destabilize domestic politics within days. No nation, however powerful, can face this challenge alone.

What is required is cross-border collaboration that is deep, structured, and sustained. We must strengthen information sharing so that emerging threats are detected early and alerts are raised before crises spread. We must work toward international standards and governance frameworks that ensure AI is used responsibly in sensitive domains, particularly in the military where miscalculation could lead to conflict. We must develop joint response mechanisms to ensure that cyber defense, counter-disinformation operations, and recovery strategies can be coordinated seamlessly. And perhaps most importantly, we must establish confidence-building measures in military applications, ensuring transparency that prevents misunderstandings and unintended escalation.

For Malaysia, this means engaging with ASEAN partners, collaborating with global institutions, and working closely with responsible technology leaders. Cross-border collaboration is not optional; it is a strategic necessity.

Part IV – The Role of Today's Exercise

This brings us to the role of today's exercise. By participating in this tabletop simulation, we are taking an important step in preparing our institutions, our defense, and our society for the realities of the AI age. Such exercises allow us to simulate crises, whether in the form of AI-powered cyberattacks on our power grids, disinformation campaigns targeting our democratic processes, or autonomous drones testing our sovereignty. They allow us to test our protocols, to examine whether agencies know their roles, their chains of command, and the sequence of actions required. Most importantly, they help us build trust among stakeholders. In a real crisis, silos are fatal. Defense, intelligence, civil society, the private sector, and international partners must act as one ecosystem, operate back-to-back, to form an intact WoGoS (Whole of Government, Whole of Society) in a wider dimension.

These scenarios are not drawn from science fiction. They are rehearsals for challenges we are very likely to face within the next decade.

Why a Tabletop Exercise is Critical

This is why today's tabletop exercise is not an academic exercise but a matter of strategic importance. Such rehearsals provide us with the chance to anticipate and simulate crises that could one day paralyze our nation or destabilize our region. They force us to ask hard but necessary questions. Do our institutions know who takes the first decision in the event of an AI-triggered crisis? Are our armed forces, cyber agencies, and civilian ministries prepared to collaborate seamlessly, without the friction of bureaucracy? How quickly can we call upon our regional partners when a crisis spills across borders?

This exercise allows us to stress-test our assumptions, identify our blind spots, and forge practical solutions. It is only through such preparations that we can strengthen our resilience against crises that will almost certainly confront us in the years ahead.

Realism in Tabletop Exercises

While tabletop exercises are designed for safety and strategic reflection, they must also embrace realism. If our scenarios are too scripted, too comfortable, or too predictable, we risk rehearsing for an ideal world rather than preparing for the messy realities of crises. Realism matters because it exposes our blind spots and compels us to face uncomfortable truths.

In real crises, time will be short, information will be incomplete, and decisions will carry grave consequences. By embedding realism into today's exercise through unpredictable injects, red-teaming adversaries, and simulating information overload we create conditions that mirror the pressures of real-world crises. This is not to discourage us but to make us sharper. Only by stress-testing our assumptions under realistic conditions can we discover flaws in our systems, improve our readiness, and build the resilience that will define success or failure when the real crisis comes.

Conclusion

Artificial Intelligence is the defining technology of our century. It has the potential to be a force multiplier for resilience and defense, or a catalyst for insecurity and crisis. The difference lies in how we prepare, how we govern, and how we collaborate across borders.

Yet the very same technology can be weaponized against us. Algorithms can be manipulated, autonomous systems can escalate conflicts without human oversight, and AI-powered disinformation can destabilize societies. Just as AI strengthens our defense, it also exposes new vulnerabilities that adversaries can exploit.

Thus, AI is not inherently good or bad, it is a double-edged sword, and the outcome depends on how wisely, responsibly, and collaboratively we employ it. Let us not underestimate the risks but let us also not ignore the opportunities. Above all, let us remember that the safety of our people, the stability of our region, and the security of our nation depend on the choices we make now.

Rear Admiral Fadhil Abdul Rahman
Director General, Cyber and Electromagnetic Defense Division
Malaysia Armed Forces

Executive summary

This tabletop exercise (TTX) brought together Malaysian policymakers, security agencies, regulators, and business representatives to simulate a four-week campaign of cyber and disinformation attacks during a politically sensitive period. The TTX was convened to test Malaysia's readiness for hybrid crises combining cyber-physical attacks and disinformation.

The objectives of the exercise were to:

- Appreciate the implications of artificial intelligence in enabling crisis escalation.
- Assess coordination mechanisms among cyber, intelligence, communications, law enforcement, defense, and diplomatic agencies.
- Examine strategies for public communication to counter disinformation.
- Evaluate the benefits and drawbacks of international partnerships.
- Formulate recommendations to strengthen national cyber resilience.

Across three escalating phases, participants were challenged to advise ministers and national agencies on urgent response measures in the face of disinformation offensives, cyber-physical disruptions, and systemic national crises.

The exercise highlighted the urgency of strengthening whole-of-government coordination, accelerating rapid public communications, and building resilience through both national mechanisms and international partnerships. While participants demonstrated creative solutions and strong inter-agency awareness, the exercise exposed gaps in technical continuity, cross-border enforcement, and public trust management.

Specifically, the table-top exercise illustrated:

- That participants adapted well to the scenarios, but responses can be in silos. Participants or groups never moved away from the individual level and can be agency centric. This could allude to the desire to keep within the roles of the TTX, despite the facilitators outlining at the beginning of the TTX that inter-agency coordination is welcome. Worryingly, the absence of interagency coordination may also indicate that there are no relationships, no partnerships or perhaps no protocols between agencies.
- Responses tend to be reactionary and focus on putting out fires, be it in the information or cyber-physical domain. There were several attempts to conduct investigations and seek the source of activities. However, there is uncertainty for further course of action after an investigation is conducted. There were questions if results of investigation and information-sharing should go through the Attorney-General Chambers to verify and advise for further attribution. There were also glaring blind spots where geopolitics is concerned.
- The ability to respond to the multi-domain environment varies and participants respond well within their jurisdiction. While one group could display wide-ranging responses covering possible support to other agencies and internal communication to strengthen resilience, others could only respond for their constituents and sectors.

Critical observations on response readiness:

Beyond individual agency capabilities, the exercise revealed three systemic challenges that may require attention:

- **Speed considerations:** current government response cycles may not align well with the velocity of AI-enabled threats. Where disinformation and cyber-physical attacks can cascade within hours, traditional inter-agency coordination processes typically operate on timescales of days or weeks. This temporal gap could represent a vulnerability that may not be fully addressed through improved communication alone.
- **Structural considerations:** while the National Security Council provides an effective escalation point, the exercise suggested that hierarchical coordination alone may be insufficient for modern hybrid threats. Agencies appear to lack the operational infrastructure - such as shared systems, joint protocols, and collaborative cultural practices - that would enable them to function as an integrated response team rather than parallel actors. The presence of appropriate agencies does not automatically enable networked collaboration.
- **Peacetime preparation:** the hesitation to coordinate during the exercise could reflect the absence of established operational relationships. Inter-agency effectiveness under crisis conditions may depend on peacetime relationship-building, joint training, and routine collaborative practices that create familiarity with integrated response approaches.

Lessons learned and recommendations:

1. There may be hesitation to pursue inter-agency collaboration in a crisis. While participants were able to adapt to a multi-domain challenge, responses do not pursue inter-agency collaboration indicating the possibility that there are no relationships, no partnerships or perhaps no protocols between agencies. It may be the burden of the highest authority – in this case the National Security Council – to drive inter-agency collaboration during the crisis. To enhance a whole-of-government approach, it is recommended for Malaysia to pursue trust-building exercises among agencies which could lead to higher comfort levels for inter-agency response in the midst of a crisis.
2. There is a need to inculcate incident response beyond reactionary mechanisms. While incident response focuses on addressing cyberattacks, there is a need to strengthen investigation and threat hunting mechanisms. Responsibilities in an incident could be diverse and may require different officers in charge of firefighting, investigations and internal resilience. Furthermore, there needs to be policy clarity for a course of action upon the completion of an investigation.
3. Policies that clarify thresholds for hybrid operations would also be useful, especially in the case of a multi-domain attack that includes disinformation campaigns and attacks on critical infrastructure. The policy could develop a traffic light protocol, especially where such campaigns could impact national interest. However, underpinning a traffic light protocol are fundamental conversations on the types of information campaigns and their impact on national security, especially to address potential gaps caused by

geopolitics. These conversations are necessary to structure response and outreach for assistance.

The tabletop exercise also presented lessons to the design which limited the learning experience.

There were time constraints to the tabletop exercise which impacted its design. While the SITREPs could illustrate the breadth of attacks, it did not allow for responses to be agile. This may have impacted the ability for certain decisions to plateau such as the decision to conduct investigations, which were established in phase 1 and abandoned in phase 2 due to a lack of response in the SITREP. The time limit also caused immersion to occur only in the latter half of phase 2. It is recommended for future tabletop exercises to take place over a day.