

**REPORT BY GENERAL MOHD AZUMI BIN MOHAMED (RETIRED)  
THE CHAIRMAN, BOARD OF DIRECTORS  
CYBERSECURITY MALAYSIA  
AT INFOFORUM UGRA 2018**

**CYBER DIPLOMACY AND MULTILATERAL COOPERATION**

1. LET ME BEGIN BY THANKING DR ALEXANDER ZHUKOV, HEAD OF INFOFORUM FOR INVITING ME.
2. THIS IS MY THIRD APPERANCE AT THE INFOFORUM. I WAS PREVILEGED TO BE HERE IN KHANTY-MANSISK LAST YEAR AND AT SHANGHAI IN 2016.
3. I FIND INFOFORUM A VERY USEFUL AND APPROPRIATE PLATFORM AND OPPURTUNITY TO ENGAGE AND INTERACT NOT ONLY OVER THE DEVELOPMENT OF ICT, BUT ALSO IN POLICY DISCUSSIONS OVER NORMS, CONFIDENCE BUILDING MEASURES, CAPACITY BUILDING WITH A VIEW TO CREATING AND BUILDING TRUST AMONGST STATES, THUS LOWERING THE RISK OF ANY ESCALATION IN THE USE OF ICTS.
4. WE ARE TODAY IN AN ERA OF COMPUTING POWER AND INFORMATION TECHNOLOGY THAT HAS EXPANDED INTO EVERY SPHERE OF OUR EXISTENCE. ITS PERVASIVENESS IN THE CRITICAL NETWORK INFRASTUCURE HAS REVOLUTIONIZED VULNERABILITIES. IT HAS ACCORDING TO

THE BOOK "WORLD ORDER" BY KISSINGER OUTSTRIPPED STRATEGY AND DOCTRINE. IN THE PAST WE TALK OF GREAT RUSSIAN STRATEGIST LIKE GENERAL ALEXANDER SUVIROV, CLAUSEWITZ BUT TODAY A LAPOP CAN PRODUCE CONSEQUENCES.

5. GOVERNMENTS HAVE ACKNOWLEDGED THE NEED TO BUILD TRUST AND ENGAGE DEEPER INTO INTERNATIONAL GOVERNANCE AND COOPERATION IN THE DEVELOPMENT OF CYBER SECURITY, GIVEN ITS CRITICAL ROLE AS ENABLERS OF ECONOMIC, POLITICAL AND SOCIAL DEVELOPEMENT AND THAT DIGITAL TECHNOLOGY HAS PROVIDED UNPRECEDENTED OPPORTUNITIES FOR GLOBAL COMMUNITIES TO UTILIZE TELECOMMUNICATIONS, INFRASTRUCTURE, COMPUTERS AND APPLICATIONS TO BOTH NATIIONAL AND INTERNATIONAL ADVANTAGES.
6. GOVERNMENTS DO RECOGNIZE THAT CYBER SECURITY FORMS AN INTEGRAL PART OF TECHNOLOGICAL PROGRESS AS WE EMBARK ON A MORE SECURED AND SAFE DIGITAL ENVIRONMENT.
7. THE HOLDING OF INFOFORUM UGRA 2018 IS TESTIMONY THAT TODAY WE ARE NOT ONLY FACED WITH ENVIRONMENTAL CONCERNS, CONFLICTS, RISKS, POVERTY, NATURAL DISASTERS BUT A CHALLENGE THAT'S HERE TO REMAIN. THE ICT4 PEACE FOUNDATION DESCRIBES THIS CHALLENGE AS AN INVASIVE, MULTI

PRONGED AND MULTI LAYERED THREAT. A MODERN DAY ARMS RACE WITHOUT VISIBLE ACTORS, WEAPONS, CHARACTERIZED BY AN ESCALATING NUMBER OF ATTACKS BOTH ON AND OFF RADAR.

8. THIS IS WELL CITED BY THE DIRECTOR TELECOMMUNICATIONS BUREAU OF THE ITU, WHO IN HIS FOREWORD TO THE GLOBAL CYBER SECURITY INDEX 2017 MADE REFERENCE TO, IN 2016 NEARLY ONE PERCENT OF ALL EMAILS SEND WERE MALICIOUS ATTACKS. THE HIGHEST RATE IN RECENT YEARS AND THE MAY 2017 MASSIVE CYBER ATTACK CAUSING MAJOR DISRUPTIONS IN OVER 150 COUNTRIES PROMPTING GREATER INTERNATIONAL COOPERATION.
9. CRITICAL INFRASTRUCTURES HAVE BECOME TARGETS FOR CYBER ATTACKS. SUCH ATTACKS AS WE HAVE WITNESSED, CAN BE VERY DEVASTATING AND IMPACTS NATIONS. IS THE INTERNATIONAL COMMUNITY DOING ENOUGH TO PREVENT OR MINIMIZE THE POTENTIAL RISKS OF AN ESCALATION OF CYBER CONFLICT?
10. MY RESPONSE TO THAT, THROUGH CONFIDENCE BUILDING MEASURES LIKE THE HOLDING OF CONFERENCES, COLLABORATION AND COOPERATION. AMONGST STATES, THROUGH BILATERAL AGREEMENTS AND MULTILATERAL AGREEMENTS AND PARTICIPATION IN INTERNATIONAL CYBER SECURITY EVENTS LIKE

INFOFORUM, TRAINING, WORKSHOPS, TECHNICAL COOPERATION (LIKE THE MALAYSIAN TECHNICAL COOPERATION PROGRAMME), CYBER SECURITY EXERCISES, INFO SHARING, ARE BUT SOME OF THE CYBER DIPLOMACY EFFORTS THAT WE CAN UNDERTAKE COLLECTIVELY TO HELP BUILD TRUST BETWEEN STATES THUS ENSURING A SAFER AND APPROPRIATE USE OF ICTS.

11. MISTRUST AND A LACK OF TRANSPARENCY WILL LEAD TO A MORE POROUS CYBER DEFENCE MECHANISM. TACKLING A GLOBAL THREAT REQUIRES A GLOBAL EFFORT, A CONTINUED PLAN OF ACTION ACTING IN CONCERT AND DIALOGUE TO FIND A COMMON GROUND IN RESPONDING TO SUCH CYBER THREATS IS A MUST.
12. WE NEED TO DEVELOP AN EFFECTIVE INTERNATIONAL RESPONSE TO CYBER THREATS. IT HAS TO BE EFFECTIVE GIVEN THAT CYBER SECURITY IS AN ECO-SYSTEM WHERE LAWS, ORGANIZATIONS, SKILLS, COOPERATION NEEDS TO BE HARMONIZED TO BE EFFECTIVE .
13. READING THE NUMEROUS FOREWORD IN THE INFOFORUM UGRA 2018 PROGRAMMES, I AM PLEASED TO NOTE OF THE REMARKS EMPHASIZING ON THE SAFER USE OF DIGITAL TECHNOLOGIES, INFOFORUM AS A UNIQUE PLATFORM TO RESOLVE ISSUES OF INTERNATIONAL AND INTER REGIONAL COOPERATION, DISCUSSING MATTERS AIMED AT PREVENTING AND NEUTRALIZING CYBER THREATS, THE

SEARCH FOR EFFECTIVE SOLUTIONS, CONSOLIDATION OF EFFORTS, STRENGTHENING INTERNATIONAL COOPERATION ARE REMINDERS OF THE NEED FOR US TO DRIVE FURTHER EFFORTS IN DEVELOPING CYBER DIPLOMACY AND CONFIDENCE BUILDING MEASURES WITH A VIEW TO MAKING THE DIGITAL WORLD A MORE SECURE AND SAFER ENVIRONMENT.

14. WE HAVE MUCH IN COMMON IN RELATION TO OUR COMMITMENT AND ENGAGEMENT TO CYBER SECURITY. THE GLOBAL CYBER SECURITY INDEX 2017, A SURVEY OF COMMITMENT AND READINESS TO CYBER SECURITY OF A 193 MEMBER COUNTRIES OF THE ITU RANKS, THE RUSSIAN FEDERATION SECOND AMONGST THE COMMONWEALTH OF INDEPENDENT STATES (CIS) AND IS ACKNOWLEDGED FOR ITS CAPACITY BUILDING, DEVELOPING CYBER SECURITY STANDARDS TO R&D. THE RUSSIAN FEDERATION IS ALSO RANKED TOP TEN GLOBALLY, AND IN THE LEADING STAGE DEMONSTRATING A HIGH COMMITMENT IN ALL PILLARS OF THE SURVEY. I AM MADE TO UNDERSTAND THAT ONE OF THE OBJECTIVES OF THE INFORMATION SECURITY AREA OF GOVERNMENTAL PROGRAMME DIGITAL ECONOMY OF THE RUSSIAN FEDERATION IS TO ENSURE THE LEADING POSITIONS FOR RUSSIA IN THE EXPORT OF INFORMATION SECURITY SERVICES AND TECHNOLOGIES, AS WELL AS THE INTEGRATION OF NATIONAL INTERESTS IN INTERNATIONAL DOCUMENT OF INFORMATION SECURITY ISSUES.

15. MALAYSIA ON THE OTHER HAND IS RANKED SECOND IN THE ASIA PACIFIC REGION AND LIKE THE RUSSIAN FEDERATION GLOBALLY TOP TEN AND IN THE LEADING STAGE OF CYBER SECURITY COMMITMENT.
  
16. OF COURSE, THE GCI DOES NOT DENY OF THE DIVIDE AND GAP IN THE LEVEL OF CYBER SECURITY ENGAGEMENT BETWEEN REGIONS AND COUNTRIES. BUT WHAT IS IMPORTANT IS THAT COUNTRIES LIKE THE RUSSIAN FEDERATION, MALAYSIA EITHER ACTING REGIONALLY OR INTERNATIONALLY CAN HELP IMPROVE THIS LEVEL OF DISPARITY AND GAP THROUGH CYBER DIPLOMACY BY ASSISTING, COLLABORATING IN THE CYBER SECURITY AGENDA OF COOPERATION AT ALL LEVELS SUCH AS CAPACITY BUILDING, ORGANIZATIONAL MEASURES, CYBER RESILIENCE WHICH IS GENERALLY LOW AND THE VARYING LEVEL OF CYBER READINESS AMONGST COUNTRIES. BESIDES THAT, POLICY PREPAREDNESS AND INSTITUTIONAL OVERSIGHT RELATING TO CYBER SECURITY ARE AREAS THAT CAN BE JOINTLY DEVELOPED.
  
17. LOOKING AT THE DIRECT CAUSE EFFECT PRINCIPLE BETWEEN THE GROWTH OF ICT AND ITS ILLICIT AND MALICIOUS USE AND EXPOSURE OF THE CYBER WORLD TO THE VARIOUS THREATS, CYBER DIPLOMACY SHOULD BE THE NORM AND CAN HELP BUILD TRUST AND TRANSPARENCY BETWEEN COUNTRIES. IN DOING SO, WE CAN HELP DEVELOP PROPER STRATEGY, AWARENESS,

CAPACITY, CAPABILITIES, KNOWLEDGE IN THE REALIZATION OF A SAFER AND APPROPRIATE USE OF ICTS AS ENABLERS OF SOCIAL, ECONOMIC AND POLITICAL DEVELOPMENT. WE HAVE TO LOOK AT THE INCREASED NEED OF INVESTMENT IN TRAINING, CAPACITY BUILDING, DEVELOPMENT ASSISTANCE TO HELP FOSTER A SAFER, SECURED AND RESILIENT CYBER SPACE.

18. SPEAKING WITH ONE MIND, THE INTERNATIONAL COMMUNITY MUST CONTINUE PUSHING FOR A CYBER DIPLOMACY AND COOPERATION AGENDA.
19. INFOFORUM UGRA 2018 CAN BE THE COMMON GROUND, DENOMINATOR AND CONSENSUS IN MITIGATING CYBER THREATS BY A CONTINUOUS AND CONCERTED INTERNATIONAL CYBER CONFLICT AGENDA. THROUGH CYBER DIPLOMACY, THE NEED TO ENGAGE IN BILATERAL, MULTILATERAL AND INTERNATIONAL COOPERATION IS TO ENHANCE CYBER SECURITY.
20. IN SO DOING, THE GLOBAL COMMUNITY CAN EFFECTIVELY STAY IN CONTACT AND TOUCH THROUGH THE SHARING OF EXPERIENCES, VIEWS AND SOLUTIONS AS CITED IN THE FOREWORD OF THIS INFOFORUM UGRA 2018. IN SUMMARY, CYBER DIPLOMACY IS DESIGNED TO REGULATE GOOD RELATIONS IN THE CYBER SPACE AND THE PROMOTION OF PEACE.

21. THE INTERNATIONAL COOPERATION THAT IS BEING ADVOCATED IS AIMED AT CULTIVATING HARMONY. AN ABSENCE OF DIPLOMACY CAN PAVE THE WAY FOR A CRISIS TO ARISE. THE WAY FORWARD, IS TO PURSUE AND BE CONTINUOUSLY ENGAGED THROUGH DIPLOMACY. WHICH CAN PREVENT A POSSIBLE CYBER CRISIS FROM ARISING AS A RESULT OF A MISCOMMUNICATION, MISTATEMENT OR MISREPRESENTATION.
22. WE NEED A GLOBAL FRAMEWORK TO ORGANIZE A CYBER ENVIRONMENT WHICH AT LEAST CHECKMATE US ON DANGERS OF CYBER ATTACKS AND CONSEQUENCES.
23. THERE ARE GOOD AND BEST PRACTICES THAT WE CAN SHARE. THERE IS STILL SPACE FOR FURTHER COOPERATION AT ALL LEVELS. IN THIS RESPECT, ASEAN OVER THE PAST YEAR, HAS BEEN HIGHLIGHTING CYBER SECURITY AS ITS AGENDA THROUGH ITS ASEAN MINISTERIAL CONFERENCE ON CYBER SECURITY STARTING WITH CAPACITY BUILDING.
24. THE CYBER THREAT LANDSCAPE IS LIKELY TO GENERATE GREATER COMPLEXITY, FURTHER ESCALATING CHALLENGES TO CYBER SECURITY. RESPONSE TO THESE CHALLENGES MUST BE COMPREHENSIVE. HENCE CYBER DIPLOMACY, CYBER NORMS AND CONFIDENCE BUILDING MEASURES NEEDS TO REMAIN EMPHASIZED AND BE



PUSHED BY THE INTERNATIONAL COMMUNITY EITHER  
BILATERAL OR REGIONAL OR MULTILATERAL.

25. THANK YOU.