Aspects juridiques et réglementaires de la sécurité des systèmes d'information

Pr. Radouane Mrabet
ENSIAS, Université Mohammed V de Rabat


radouane.mrabet@gmail.com


@radouane_mrabet

Année Universitaire 2015-2016

C2 : Cybercriminalité

Global Cybersecurity Index – GCI

Année Universitaire 2015-2016

Global Cybersecurity Index GCI

- L'Indice de cybersécurité évalue le niveau d'engagement des États dans les cinq domaines d'activités suivants:
  - cadre juridique,
  - mesures techniques,
  - structures organisationnelles,
  - renforcement des capacités, et
  - coopération internationale.
- Le GCI ne cherche pas à prouver l'efficacité ou le succès d'une mesure en particulier, mais simplement l'existence des structures nationales en place pour mettre en œuvre et promouvoir la cybersécurité.

Pays	Indice	Classement mondial
Etats-Unis d'Amérique*	0,824	1
Canada*	0,794	2
Australie*	0,765	3
Malaisie	0,765	3
Oman	0,765	3
Nouvelle-Zélande*	0,735	4
Norvège*	0,735	4
Colombie	0,588	9
Danemark*	0,588	9
Egypte	0,588	9
France*	0,588	9
Maurice	0,588	9
Espagne*	0,588	9
Italie	0,559	10
Maroc	0,559	10
Ouganda	0,559	10
Azerbaïdjan	0,529	11
Pologne*	0,529	11
Rwanda	0,529	11
Tunisie	0,529	11
République tchèque	0,500	12
Géorgie	0,500	12
Russie*	0,500	12

Etats arabes	Juridique	Technique	Organisationnel	Renforcement des capacités	Coopération	Indice	Classement régional
Oman	0,7500	0,6667	1,0000	0,7500	0,6250	0,7647	1
Qatar	0,7500	0,8333	0,5000	0,6250	0,5000	0,6176	2
Egypte	0,5000	0,5000	0,3750	1,0000	0,5000	0,5882	3
Maroc X	0,5000	0,6667	0,7500	0,5000	0,3750	0,5588	4
Tunisie	1,0000	0,5000	0,6250	0,2500	0,5000	0,5294	5
Soudan	0,7500	0,5000	0,5000	0,2500	0,3750	0,4412	6
Emirats arabes unis*	0,7500	0,3333	0,2500	0,5000	0,1250	0,3529	7
Bahreïn	0,7500	0,1667	0,1250	0,3750	0,2500	0,2941	8
Libye	0,2500	0,3333	0,3750	0,1250	0,3750	0,2941	8
Arabie saoudite*	0,7500	0,3333	0,1250	0,3750	0,1250	0,2941	8
Jordanie	0,5000	0,0000	0,5000	0,0000	0,1250	0,2059	9
Algérie	0,7500	0,0000	0,0000	0,1250	0,2500	0,1765	10
Syrie	0,2500	0,3333	0,1250	0,1250	0,1250	0,1765	10
Mauritanie	0,2500	0,1667	0,2500	0,0000	0,1250	0,1471	11
Etat de Palestine*	0,2500	0,0000	0,3750	0,1250	0,0000	0,1471	11
Liban	0,0000	0,0000	0,0000	0,2500	0,1250	0,0882	12
Djibouti	0,2500	0,0000	0,0000	0,0000	0,1250	0,0588	13
Koweït*	0,0000	0,0000	0,0000	0,1250	0,1250	0,0588	13
Yémen*	0,2500	0,0000	0,0000	0,0000	0,1250	0,0588	13
Comores	0,0000	0,0000	0,0000	0,0000	0,1250	0,0294	14
Iraq*	0,0000	0,0000	0,0000	0,0000	0,1250	0,0294	14
Somalie	0,0000	0,0000	0,0000	0,1250	0,0000	0,0294	14

** Résultats tirés des données secondaires*

Le Maroc 4ème dans le monde arabe

@radouane_mrabet

Afrique	Juridique	Technique	Organisationnel	Renforcement des capacités	Coopération	Indice	Classement régional
Maurice	0,7500	0,6667	0,6250	0,5000	0,5000	0,5882	1
Ouganda	0,7500	0,5000	0,8750	0,2500	0,5000	0,5588	2
Rwanda	1,0000	0,5000	0,5000	0,3750	0,5000	0,5294	3
Nigéria	0,2500	0,3333	0,5000	0,5000	0,5000	0,4412	4
Cameroun	0,7500	0,5000	0,3750	0,5000	0,1250	0,4118	5
Kenya	1,0000	0,3333	0,2500	0,2500	0,5000	0,4118	5
Afrique du Sud	0,2500	0,5000	0,6250	0,2500	0,2500	0,3824	6
Burkina Faso	0,0000	0,5000	0,7500	0,0000	0,2500	0,3235	7
Ghana*	0,7500	0,3333	0,2500	0,2500	0,1250	0,2941	8
Togo	0,0000	0,3333	0,3750	0,2500	0,2500	0,2647	9
Côte d'Ivoire	0,7500	0,3333	0,1250	0,1250	0,1250	0,2353	10
Libéria	0,0000	0,0000	0,2500	0,3750	0,2500	0,2059	11
Tanzanie	0,5000	0,3333	0,0000	0,1250	0,2500	0,2059	11
Bénin*	0,5000	0,0000	0,2500	0,1250	0,1250	0,1765	12
Botswana	0,7500	0,1667	0,2500	0,0000	0,0000	0,1765	12
Malawi	0,0000	0,0000	0,1250	0,3750	0,2500	0,1765	12
Sénégal*	1,0000	0,0000	0,1250	0,0000	0,1250	0,1765	12
Zambie	0,2500	0,3333	0,1250	0,1250	0,0000	0,1471	13
Burundi	0,2500	0,0000	0,1250	0,1250	0,1250	0,1176	14
Seychelles*	0,7500	0,0000	0,0000	0,0000	0,1250	0,1176	14
Angola*	0,5000	0,0000	0,0000	0,0000	0,1250	0,0882	15
Gambie	0,5000	0,0000	0,1250	0,0000	0,0000	0,0882	15

Le Maroc 3ème en Afrique

@radouane_mrabet

Comment est calculé le GCI ?

1. Cadre juridique	**4**
A. Législation pénale	2
B. Réglementation et conformité	2
2. Mesures techniques	**6**
A. Centres de veille, d'alerte et de réponse aux incidents informatiques (CERT/CIRT/CSRIT)	2
B. Normes	2
C. Certification	2
3. Structures organisationnelles	**8**
A. Politique	2
B. Feuille de route relative à la gouvernance	2
C. Organisme responsable	2
D. Evaluations comparatives nationales	2

Comment est calculé le GCI ?

4. renforcement des capacités;	**8**
A. Normalisation	2
B. Développement des compétences des ressources humaines	2
C. Certification professionnelle	2
D. Certification des organismes	2
5. Coopération internationale	**8**
A. Coopération entre Etats	2
B. Coopération entre organismes	2
C. Partenariats public-privé	2
D. Coopération internationale	2

Cadre juridique

- Les critères de mesure du cadre juridique peuvent être l'existence et le nombre d'institutions et de cadres juridiques relatifs à la cybersécurité et à la cybercriminalité. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

  A. Législation pénale

  B. Réglementation et conformité

Cadre juridique
A. Législation pénale

- On entend par législation anti-cybercriminalité l'ensemble des lois couvrant l'accès, l'ingérence et l'interception illicites (sans en avoir le droit) en rapport avec le matériel informatique, les systèmes et les données.
- La réglementation peut relever de l'un des trois niveaux suivants:
  - aucune,
  - partielle : correspond à la simple insertion d'une mention en rapport avec l'informatique dans une loi ou un code pénal existant(e), se limitant à étendre au cyberespace les notions de fraude ou de contrefaçon ou bien de surveillance et de vol, par exemple.
  - Exhaustive : correspond à la promulgation d'une loi spéciale portant sur des aspects spécifiques de la criminalité informatique.

Cadre juridique
B. Réglementation et conformité

- On entend par réglementation relative à la cybersécurité la législation couvrant la protection des données, la notification des infractions et les obligations en matière de certification/normalisation.
- La réglementation peut relever de l'un des trois niveaux suivants:
  - aucune,
  - partielle : correspond à l'insertion d'une mention en rapport avec l'informatique dans une loi pénale ou civile existante ou nouvelle, de façon que ladite loi s'applique au cyberespace dans une réglementation sans relation spécifique ou exclusive avec la cybersécurité
  - Exhaustive : correspond à la promulgation d'une loi ou d'une directive spéciale exigeant spécifiquement le respect de la cybersécurité.

Mesures techniques

- Les critères d'évaluation des mesures techniques peuvent être l'existence et le nombre d'institutions et de cadres techniques en rapport avec la cybersécurité approuvés ou créés par l'Etat.
- Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

  A. Centres de veille, d'alerte et de réponse aux incidents informatiques (CERT/CIRT/CSRIT)

  B. Normes

  C. Certifications

Mesures techniques

A. Centres de veille, d'alerte et de réponse aux incidents informatiques (CERT/CIRT/CSRIT)

- Création de centres de veille, d'alerte et de réponse aux incidents informatiques de type CIRT (équipe d'intervention en cas d'incident informatique), CERT (équipe d'intervention d'urgence en cas d'incident informatique) ou CSIRT (équipe d'intervention en cas d'incident relatif à la sécurité informatique), capables d'identifier les cybermenaces, de les prévenir, d'y répondre, de les gérer et de renforcer la sécurité du cyberespace dans le pays.
- L'Etat doit associer cette capacité à la collecte de ses propres renseignements et ne pas se fier entièrement au signalement de seconde main des incidents de sécurité par les membres du CIRT ou d'autres sources.
- Le classement du niveau de développement dépendra de l'existence ou de l'absence de centres nationaux et d'un mandat légal.

Mesures techniques
B. Normes

- Cet indicateur mesure l'existence d'un ou de plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant l'application des normes internationales en matière de cybersécurité dans le secteur public (administrations) et dans l'infrastructure vitale (même si elle est gérée par le secteur privé).
- Ces normes incluent, sans s'y limiter, celles élaborées par les organismes suivants: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.

Mesures techniques
C. Certifications

- Cet indicateur mesure l'existence d'un ou de plusieurs cadres approuvés (ou ratifiés) par le gouvernement concernant la certification et l'accréditation d'organismes nationaux (administrations) et de professionnels du secteur public sur la base de normes internationales en matière de cybersécurité.

Mesures techniques
C. Certifications

- Ces certifications, accréditations et normes sont, entre autres, les suivantes: connaissance de la sécurité dans le nuage informatique (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Conseil de l'Europe), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), (pas de suggestion) Certification, Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), PRMIA (Professional Risk Managers International Association), PMP (Project Management Institute), etc.

Structures organisationnelles

- La mise en œuvre d'une initiative nationale, quelle qu'elle soit, requiert des mesures organisationnelles et procédurales. L'Etat doit fixer un objectif stratégique général donnant lieu à l'établissement d'un plan complet de mise en œuvre, d'exécution et de mesure. Des structures telles que des organisations nationales doivent être constituées pour appliquer la stratégie et évaluer la réussite ou l'échec du plan.

Structures organisationnelles

- Les critères de mesure des structures organisationnelles sont l'existence et le nombre des institutions et des stratégies organisant le développement de la cybersécurité au niveau national.
- Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

  A. Politique

  B. Feuille de route relative à la gouvernance

  C. Organisme responsable

  D. Évaluations comparatives nationales

Structures organisationnelles
A. Politique

- L'élaboration d'une politique de promotion de la cybersécurité est reconnue comme une priorité majeure.
- La stratégie nationale de sécurité des réseaux et des systèmes d'information doit assurer la résilience et la fiabilité de l'infrastructure informatique et viser à garantir la sécurité des citoyens, protéger les ressources physiques et intellectuelles des citoyens, des organisations et de l'Etat, empêcher les cyberattaques contre les infrastructures vitales, limiter les dégâts dus aux cyberattaques et raccourcir les délais de rétablissement.

Structures organisationnelles
A. Politique

- Les politiques en matière de stratégies nationales de cybersécurité ou de plans nationaux pour la protection des infrastructures informatiques sont celles officiellement définies et approuvées par les Etats.
- Elles peuvent comprendre les engagements suivants:
  - désigner clairement des responsables de la cybersécurité à tous les niveaux de gouvernement (local, régional et fédéral ou national) dotés de rôles et de responsabilités clairement définis,
  - s'engager clairement dans une cybersécurité publique et transparente et encourager la participation du secteur privé et les partenariats public-privé dans le cadre des initiatives de promotion de la cybersécurité placées sous l'égide des pouvoirs publics.

Structures organisationnelles

B. Feuille de route relative à la gouvernance

- En général, la feuille de route relative à la gouvernance de la cybersécurité est définie par la politique nationale en matière de cybersécurité et désigne les principales parties prenantes.

Structures organisationnelles
C. Organisme responsable

- L'organisme responsable de la mise en œuvre de la stratégie/politique nationale en matière de cybersécurité peut comprendre :
  - des comités permanents,
  - des groupes de travail officiels,
  - des conseils consultatifs et
  - des centres interdisciplinaires.
- La plupart des organismes nationaux seront directement responsables des systèmes de veille et d'alerte ainsi que de réponse aux incidents, mais aussi de l'élaboration des structures organisationnelles requises pour coordonner les réponses aux cyberattaques.

Structures organisationnelles
D. Évaluations comparatives nationales

- Cet indicateur mesure l'existence d'exercices d'évaluation comparative nationaux ou sectoriels officiels ou d'un référentiel servant à mesurer le développement de la cybersécurité.
- Par exemple, une norme de cybersécurité nationale basée sur la norme ISO/CEI 27002-2005 peut aider les Etats à répondre à des exigences spécifiées en matière de cybersécurité.

Renforcement des capacités

- Le renforcement des capacités est intrinsèque aux trois premières catégories de mesure (juridique, technique et organisationnelle).
- Le cadre de renforcement des capacités visant à promouvoir la cybersécurité doit inclure la sensibilisation et l'existence de ressources. Le renforcement des capacités humaines et institutionnelles est nécessaire pour améliorer les connaissances et le savoir-faire dans tous les secteurs, appliquer les solutions les mieux adaptées et promouvoir un niveau de compétence optimal chez les professionnels. Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

  A. Normalisation

  B. Développement des compétences des ressources humaines

  C. Certification professionnelle

  D. Certification des organismes

Renforcement des capacités
A. Normalisation

- Il s'agit de connaitre les éventuels programmes/projets nationaux ou sectoriels officiels de recherche et développement axés sur les normes, les bonnes pratiques et les lignes directrices en matière de cybersécurité applicables au secteur privé ou public.

Renforcement des capacités
B. Développement des compétences des ressources humaines

- Le développement des compétences des ressources humaines doit comprendre les efforts déployés par les Etats pour promouvoir des campagnes de publicité à grande échelle visant à toucher le plus grand nombre de personnes possible, mais aussi s'appuyer sur les ONG, les institutions, les organisations, les FSI, les bibliothèques, les organisations du commerce locales, les centres communautaires, les revendeurs d'informatique, les collèges, les programmes d'éducation pour adultes, les écoles et les organisations parents-enseignants pour faire passer les messages relatifs à un comportement sûr en ligne.

Renforcement des capacités
B. Développement des compétences des ressources humaines

- Il s'agir de connaitre les éventuels programmes éducatifs et professionnels nationaux ou sectoriels officiels de sensibilisation du grand public (par exemple, jour, semaine ou mois de sensibilisation nationale à la cybersécurité), promotion de cours sur la cybersécurité dans l'enseignement supérieur (technique, sciences sociales, etc.) et promotion de la certification des professionnels dans le secteur public ou privé.

Renforcement des capacités
C. Certification professionnelle

- Les critères de mesure de cet indicateur de performance peuvent être le nombre de professionnels du secteur public certifiés conformément aux normes internationales en matière de programmes de certification.

Renforcement des capacités
D. Certification des organismes

- Les critères de mesure de cet indicateur de performance peuvent être le nombre d'organismes du secteur public et d'administrations certifiés conformément à des normes internationales.

Coopération internationale

- Les critères de mesure de la coopération nationale et internationale peuvent être l'existence et le nombre de partenariats, de cadres coopératifs et de réseaux de partage d'informations.
- Le sous-groupe d'indicateurs de performance de cette catégorie est le suivant:

  A. Coopération entre Etats

  B. Coopération entre organismes

  C. Partenariats public-privé

  D. Coopération internationale

Coopération internationale
A. Coopération entre Etats

- La coopération entre Etats fait référence à tout partenariat national ou sectoriel officiel ayant pour objet le partage des ressources en matière de cybersécurité avec d'autres Etats (partenariats bilatéraux ou multilatéraux de coopération ou d'échange d'informations, d'expertise, de technologie et/ou de ressources). Elle comprend aussi des initiatives régionales telles que (entre autres) celles mises en œuvre par l'Union européenne, le Conseil de l'Europe, le G8, l'APEC (Asian Pacific Economic Cooperation), l'OEA (Organisation des Etats américains), l'ANASE (Association des nations de l'Asie du Sud-Est), la Ligue arabe, l'Union africaine, la SCO (Shanghai Cooperation Organization) et les NOG (Network Operations Groups, Groupes opérationnels de réseaux), etc.

Coopération internationale
B. Coopération entre organismes

- On entend par coopération entre organismes tout programme national ou sectoriel officiel de partage des ressources en matière de cybersécurité (personnel, processus, outils) au sein du secteur public (partenariats officiels en vue de la coopération ou du partage d'informations, d'expertise, de technologie et/ou de ressources entre départements et organismes, par exemple). Elle comprend des initiatives et des programmes entre différents secteurs (forces de l'ordre, armée, santé, transport, énergie, gestion des déchets et de l'eau, etc.) ainsi qu'au sein des départements/ministères (autorités fédérales/locales, ressources humaines, service informatique, relations publiques, etc.). Veuillez préciser les éventuels programmes nationaux ou sectoriels officiels de partage des ressources en matière de cybersécurité au sein du secteur public.

Coopération internationale
C. Partenariats public-privé

- On entend par partenariats public-privé (PPP) les initiatives associant le secteur public et le secteur privé.
- Les critères de mesure de cet indicateur de performance peuvent être le nombre de PPP nationaux ou sectoriels officiels de partage des ressources en matière de cybersécurité (personnel, processus, outils) entre le secteur public et le secteur privé (partenariats officiels pour la coopération ou l'échange d'informations, d'expertise, de technologie et/ou de ressources, par exemple).

Coopération internationale
D. Coopération internationale

- Cet indicateur de performance mesure la participation officielle à des plates-formes et des forums internationaux sur la cybersécurité. Ces initiatives de coopération comprennent, entre autres, celles menées par l'Assemblée générale des Nations Unies, l'Union internationale des télécommunications (UIT), Interpol/Europol, l'Organisation pour la coopération et le développement économiques (OCDE), l'Office des Nations Unies contre la drogue et le crime (UNODC), l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice (UNICRI), l'ICANN (Internet Corporation for Assigned Names and Numbers), l'Organisation internationale de normalisation (ISO), la Commission électrotechnique internationale (CEI), l'IETF (Internet Engineering Task Force), FIRST (Forum for Incident Response and Security Teams).

Morocco (0,5)

1 LEGAL MEASURES

1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

-Penal Code.

1.2 REGULATION AND COMPLIANCE

Specific legislation and regulation related to cybersecurity has been enacted through the following instruments:

-Law on Personal Data Protection

-Law on Online Consumer Protection

-Law on Electronic Transfer of Legal Information.

Morocco (0,6667)

2 TECHNICAL MEASURES

2.1 CIRT

Morocco has established an official recognized national CIRT (maCERT).

2.2 STANDARDS

Morocco has an officially recognized national (and sector specific) cybersecurity framework for implementing internationally recognized cybersecurity standards through the National Strategy for Information Society and Digital Economy and National Strategy of Cybersecurity.

2.3 CERTIFICATION

Morocco has an officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals. The framework is called the Project of professional master for training and certification of professionals in the public sector.

Morocco (0,75)

3 ORGANIZATION MEASURES

3.1 POLICY

Morocco has an officially recognized national cybersecurity strategy through the National Strategy of cybersecurity and National Strategy for Information Society and Digital Economy (Digital Morocco 2013).

3.2 ROADMAP FOR GOVERNANCE

The national cybersecurity strategy provides a national governance roadmap for cybersecurity in Morocco.

3.3 RESPONSIBLE AGENCY

The General Directorate of Information Security Systems under the Administration of National Defense is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap.

3.4 NATIONAL BENCHMARKING

Morocco has officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development. These include a project for identification and classification of national information systems and another project for measuring the level of maturity of these systems.

Morocco (0,5)

4 CAPACITY BUILDING

4.1 STANDARDISATION DEVELOPMENT

Morocco does not have any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

4.2 MANPOWER DEVELOPMENT

Actions 50 to 53 of the national strategy “Digital Morocco 2013” are related to cybersecurity trainings and awareness programs. Thus as part of the national cybersecurity strategy, most scientific and technical schools and universities in Morocco integrate into their curriculum, courses in cybersecurity to meet the growing demand for skills in systems information security at national level.

4.3 PROFESSIONAL CERTIFICATION

Morocco has 69 public sector professionals certified under internationally recognized certification programs in cybersecurity.

4.4 AGENCY CERTIFICATION

Morocco has 7 government and public sector agencies certified under internationally recognized standards in cybersecurity.

Morocco (0,375)

5 COOPERATION

5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders or with other nation states, Morocco has officially recognized partnerships with the following organizations:

-ITU -South Korea

-Cybersecurity Malaysia

-FIRST -France.

5.2 INTRA-AGENCY COOPERATION

Morocco does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public sector

5.3 PUBLIC SECTOR PARTNERSHIP

Morocco does not have any officially recognized national or sector-specific programs for sharing cybersecurity assets within the public and private sector.

5.4 INTERNATIONAL COOPERATION

Morocco is a member of the ITU-IMPACT initiative and has access to relevant cybersecurity services. Morocco participated in the ITU-IMPACT Cyber Drill in Muscat, Oman in October, 2013. Morocco participated in the Applied Learning for Emergency Response Teams (ALERT) in Amman, Jordan in July, 2013 (15-17th October 2013). Morocco also participated in the ALERT in Muscat, Oman in October, 2013 (22-24th October 2013). maCERT is a member of FIRST.

Merci pour votre attention

Pr. Radouane Mrabet

ENSIAS, Université Mohammed V de Rabat

radouane.mrabet@gmail.com

@radouane_mrabet