**Groupe de recherche Sécurité et Gouvernance (GRSG)**

**Le cyberespace : enjeux, vulnérabilités et nouvelles menaces des sociétés contemporaines**

**Journée d’étude organisée par le**

***Groupe de recherche Sécurité et Gouvernance***

**Université Toulouse I-Capitole**

**Salle capitulaire du PRESS (15 rue des Lois)**

**Jeudi 29 novembre 2012**

Le cyberespace est un terrain similaire à la terre, à la mer et à l’espace aérien et extra-atmosphérique. Il est délimité par l’utilisation des systèmes électroniques et l’emploi du spectre électromagnétique. C’est un nouveau champ de bataille qui doit être défendu car il s’y déroule une activité conflictuelle assimilée à la guerre, une cyberguerre, une guerre cybernétique, une guerre informatique qui utilise des ordinateurs et internet. On ne peut donc plus concevoir de conflit militaire sans attaques sur les systèmes d’information. Ce qui semblait relever de la science fiction où le scénario montre le blocage des moyens informatiques et donc des centres de commandement ou de transmissions d’informations par des virus informatiques : véritable arme nouvelle, est redouté des Etats et des entreprises. Le virus ou le piratage peuvent produire l’arrêt, le sabotage d’infrastructures sensibles comme les moyens de transport, les centrales électriques, les systèmes de distribution d’eau, les oléoducs, les pétroliers…ou pénétrer les sites des bourses, des banques, des hôpitaux, des médias et déstabiliser ainsi l’économie et la société. Les Etats-Unis ont déjà réagi, considérant qu’une attaque informatique était une véritable déclaration de guerre provoquant une riposte militaire. Ils investissent dans la cybertechnologie. Mais à condition de pouvoir définir l’agresseur et sa provenance géographique. Il y a déjà des exemples d’attaques contre des Etats telle l’Estonie qui, en 2007, a subi la première offensive cybernétique de type étatique ou la Georgie; lors de la guerre d’Ossétie du sud, les armées géorgienne et russe ont mené la guerre informatique. En 2009, le ministère de la défense français et la Marine furent la cible d’attaques de leurs réseaux informatiques. L’année suivante, ce fut au tour du ministère de l’économie et des finances dans le cadre de la préparation de la présidence française du G8 et du G20. Les grandes entreprises telles AREVA, Airbus et Astrium furent l’objet d’intrusion informatique à des fins d’espionnage. Et dans un ouvrage récent, *les guerres secrètes du Mossad*, Yvonnick Denoël montre comment le service israélien a retardé le programme nucléaire iranien par des sabotages de centrifugeuses d’enrichissement de l’uranium par le virus Stuxnet à la conception duquel ont participé les Etats-Unis. Cela n’est qu’un épisode d’un bras de fer, véritable cyber-intifada ou cyber-djihad que se livrent Israël et le monde arabe.

Là se trouvent les nouvelles menaces du monde contemporain auxquelles répond la cybersécurité qui est la protection des systèmes d’information contre les attaques des pirates et autre vol de données sensibles qui intéresse au plus haut point les grands groupes de la défense lesquels investissent sur ce nouveau marché. Le récent rapport d’information du sénateur Jean-Marie Bockel sur *la cyberdéfense* dresse un état les lieux au niveau mondial, il souligne les insuffisances et les retards en France comme au sein de l’Union européenne face aux compétiteurs anglo-saxons et asiatiques.

Cette journée d’études organisée dans le cadre du Master2 : Relations internationales et politique de sécurité du GRSG, vise à appréhender quelques aspects de ces enjeux et menaces. Il

L’agenda de la journée d’étude est prévu comme suit :

**9 h**

**Ouverture de la journée par** **BRUNO SIRE**, **président d’Université de Toulouse1-Capitole**

**1ère séance**

**Sous la présidence de MICHEL LOUIS MARTIN**, ***professeur et directeur du GRSG***

9h10 : « Le *Libre blanc sur la défense et la sécurité nationale* de 2008 ou la stratégie d’Etat de défense et de protection dans le domaine du cyberespace », Martine Cuttier, professeur d’histoire, GRSG-UTI-Capitole, GRHI-UTM, IEP.

9h30 : « La cyber défense, une urgence nationale », Jean-Marie Bockel, ancien ministre et sénateur du Haut-Rhin.

9h50 : Discussion

10h20 : Pause

**Reprise sous la présidence de Sandra Joffroy, *maître de conférences, université Toulouse3, Paul Sabatier***

10h40 : « Les problèmes de l’évolution des systèmes d’information », Gilles Soulet, adjoint sécurité du directeur du système d’information, CNES, Toulouse

11h : « La cyber criminalité ou les risques informatiques », Major Fabrice Crasnier, gendarmerie de Midi-Pyrénées et Philippe Truillet, maître de conférence en informatique (IRIT), université Toulouse3, Paul Sabatier

11h20 : « La sécurité informatique », Jean-Marc Dubarry-Barbe, directeur d’Armance intelligence

11h40 : Discussion

12h30 : Déjeuner

**14h30**

**2e séance**

**Sous la présidence d’ANNE-MARIE SAUTEREAU**, ***professeur des universités et présidente de l’AR-IHEDN Toulouse Midi-Pyrénées***

14h40 : « Cyber conflit et cyber pouvoir, les enjeux nationaux et internationaux de la maîtrise de la cyber sécurité », professeure Solange Ghernaouti, directrice du Swiss cybersecurity advisory and reserach group, University of Lausanne

15h : « Le cyberespace : un cyber farwest ? », colonel Alain Sevilla, commandant en second de la région de gendarmerie de Franche Comté

15h20 : Discussion

15h40 : Pause

**Reprise sous la présidence de Jean-Pierre Marichy, *professeur émérite des universités, GRSG***

16h : « La cyber technologie et les cyber armes, fin de la guerre ou révolution dans l’art de la guerre ? », général de brigade Patrice Paulet, commandant de la 11e Brigade parachutiste, Toulouse

16h20 : « Cyberespace, guerre et contre-guerre, quand il est question d’information », professeur Claude Delesse, Bordeaux Business School

16h 40: « Les opérations militaires dans le cyberespace », Alain Bergeaud, consultant aéronautique et défense.

17h-18h : Discussion et clôture des débats