RELATÓRIO PARCIAL DE INICIAÇÃO CIENTÍFICA

PIBIC-CEPE

Cybersegurança

Estudante: Daniela Rocha

Relações Internacionais - 5° Período

Orientadora: Profª Drª. Salete Oliveira

2012

DEPARTAMENTO DE POLÍTICA

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

Sumário

1. RESUMO

A pesquisa pretende mostrar as procedências do conceito de cyberwar, e assim, de segurança cibernética, ao apresentar acontecimentos e o impacto dessa nova forma de guerra no cenário mundial. Após delimitar bem tal conceito, será feito um levantamento da estrutura burocrática governamental voltada para a área de segurança cibernética no Brasil e também nos Estados Unidos, juntamente com o levantamento, descrição e análise de tratados como o Acordo de Não Agressão por Armas de Informação firmado entre Brasil e Rússia, e a Organização de Cooperação de Xangai. Por fim, haverá o levantamento dos jogos chamados *serious games*, com destaque para o *Global Conflicts*, utilizados para educar e aproximar a população civil das guerras.

1.2. APRESENTAÇÃO

Segurança Cibernética é primordial, por ser um pressuposto para a manutenção das estruturas críticas dos países (entendidas por atividades que se prejudicadas, geram impactos sociais, econômicos e políticos, sem contar internacionais – tal como saúde, energia, defesa, transporte, telecomunicações e informação). O desenvolvimento de tecnologias alterou, durante o século 20, a forma de se fazer guerra. Instrumentos desde a Internet até os modernos jogos eletrônicos de recrutamento passam pelo curso de avanços e ajustes bélicos.

Segundo o Conselho de Segurança Nacional russo, o Brasil faz parte dos 16 países capazes de se valer de ataques cibernéticos e já é estimado que, no país, há cerca de 2000 ataques a grandes redes do governo por hora, com a finalidade de roubar dados e informações. Portanto, a segurança cibernética já é tida como função estratégica do Governo (http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=22683&sid=18).

Observa-se o surgimento de tratados e programas internacionais relativos ao debate, e já se aproxima de um fortalecimento em nível nacional e internacional de cooperação técnica, por exemplo, o tratado firmado entre Brasil e Rússia, em maio de 2010, chamado de "Acordo de Não Agressão por Armas de Informação" que estabelece trocas de informação usadas na capacitação de pessoal e a realização de ações conjuntas de guerra cibernética.

Este acordo é um dos pioneiros da área, só existindo semelhante o Acordo de Cooperação de Shangai, que deu origem à Organização para Cooperação de Xangai, em 15 de junho de 2001. Foram definidas novas linhas

de pensamento e ação, como, por exemplo, uma estrutura antiterror, implementada a Convenção de Xangai para Combater o Terrorismo, Separatismo e Extremismo e um acordo para combater o tráfico de drogas na região da Ásia central. Por fim, o que faz do tratado inovador, são as medidas preventivas contra o terrorismo cibernético.

O Brasil vem se destacando quando se trata de segurança cibernética. O país já foi convidado para grandes discussões e é cotado como futuro membro do grupo relacionado ao assunto na OCDE (Organização para Cooperação e Desenvolvimento Econômico). Entre os países latinos-americanos, foi o primeiro convidado a participar de discussões do Department of Homeland Security, dos Estados Unidos.

O principal objetivo desta pesquisa é analisar e apresentar os movimentos que surgem junto à nova demanda por segurança cibernética, apontando as principais medidas e tratados em âmbito global e especificamente no caso do Brasil. O projeto de pesquisa faz parte do Projeto Temático Fapesp *Ecopolítica: governamentalidade planetária, novas institucionalizações e resistências na sociedade de controle*, que aborda a análise genealógica do poder e tem como objetivo principal demarcar a passagem do controle da vida da população (biopolítica) para o controle da vida no planeta (ecopolítica).

A primeira parte da pesquisa abordou dois de quatro fluxos dentro da pesquisa: a procedência do conceito de cybersegurança e as estruturas burocráticas brasileira e americana destinadas à mesma. Anteriormente apresentei os fluxos iniciais, que estão presentes nesse relatório, e adicionalemente neste relatório, concluo minha pesquisa ao mapear e descrever tratados voltados para o campo da segurança cibernética. Em

primeiro lugar, usarei o exemplo da Organização de Cooperação de Xangai, pioneira em discussões acerca do tema. E em seguida, mostrarei como a questão está sendo abordada no Brasil, apresentando diversos acordos firmados entre Brasil e Rússia, que formam o Acordo de Não-Agressão por Armas de Informação. Por fim, pretendo mostrar como os novos conflitos tecnológicos mudaram a abordagem, por parte dos Estados, dos cidadãos e potenciais *cyberwarriors*, usando como exemplo os *serious games*.

2. RELATÓRIO DE ATIVIDADES

2.1. Objetivos alcançados e alterações no projeto inicial

Nessa segunda parte da pesquisa, pretende-se mostrar as implicações dos novos tipos de conflitos cibernéticos no cenário internacional. Foi realizada a pesquisa e mapeamento das funções da Organização de Cooperação de Xangai, pioneira na discussão de crimes cibernéticos, e do Acordo de Não-Agressão por Armas de Informação, integrante da Organização, firmado entre Brasil e Rússia em 2010. No site oficial do Itamaraty, não encontrei o segundo acordo integralmente, mas sim uma série de acordos firmados na ocasião, referentes à proteção de informação e cooperação para a superação destes novos desafios.

No site do Ministério das Relações Exteriores russo, ao buscar documentos pelas palavras chave "Brazil", "tecnology", "cyber crime" e "information weapons", não há registro de documentos. Já no site da Organização de Cooperação de Xangai encontrei a pauta da reunião em que se decidiu colocar o crime organizado e tráfico de drogas em sua agenda de segurança, e as respectivas medidas, porém de forma genérica e sem maiores informações sobre a cybersegurança em si.

Os novos tratados e acordos, firmados multilateralmente, em conjunto com a adaptação de estruturas burocráticas de países como Brasil e Estados

Unidos, mostram como a *cyberwar* já faz parte das agendas de segurança internacional em diversos países. Tais inovações são uma resposta pontual a este conflito pós-moderno, explicado por Frédéric Gros, dentro dos Estados de violência.

Em seguida, foi feito o levantamento dos chamados *serious games*, com ênfase no jogo Global Conflicts, que possui versão brasileira. Os novos jogos de guerra têm como propósito treinar os jogadores a como trabalhar em grupo em situações de conflito e guerras, e também desenvolver certas capacidades específicas. São a mais nova ferramenta de recrutamento dos exércitos nacionais.

2.2. Sistemática adotada pela orientadora e atividades

Durante o segundo semestre de 2011 realizei um programa de mobilidade, pela PUC-SP, na Universidade de Coimbra. Dessa forma, não pude comparecer às reuniões do projeto temático *Ecopolítica: governamentalidade planetária, novas institucionalizações e resistências na sociedade de controle* ou participar dos seminários apresentados ao longo do período.

No início da iniciação científica, foram delimitados, em conjunto com minha orientadora Profª. Drª. Salete de Oliveira e pelo Prof. Dr. Thiago Moreira de Souza Rodrigues, quatro movimentos dentro da pesquisa: procedências do conceito de cyberwar, o levantamento e descrição da estrutura burocrática

governamental para a área de cybersegurança no Brasil e nos Estados Unidos, o levamentamento dos "serious games"/"war games", e o levantamento e descrição dos acordos de cooperação Brasil-Rússia para cybersegurança e da Organização para Cooperação de Xangai. Mesmo à distância, continuei a pesquisar os últimos dois movimentos pendentes, que serão abordados no presente relatório.

2.3. Dificuldades encontradas e estratégias para superá-lãs

A maior dificuldade encontrada na segunda parte da pesquisa foi referente ao Acordo entre Brasil e Rússia, visto que no site do Itamaraty ele se encontra fragmentado e diversos acordos acerca do mesmo tema, e não está descrito de forma clara.

Novamente, como no primeiro momento da iniciação científica, encontrei dificuldade em relação ao material de pesquisa. Como o tema é atual, a maior parte das fontes era de artigos encontrados na Internet, ou então livros que não estavam disponíveis na biblioteca da PUC-SP ou da USP. Com a ajuda do professor Thiago Moreira de Souza Rodrigues, que me indicou alguns livros referentes ao tema e – juntamente com minha contínua pesquisa por eventos e congressos acerca do tema – atualizei-me sobre os mesmos. Foi possível reunir uma fonte bibliográfica concisa, além da netnográfica.

3. RELATÓRIO CIENTÍFICO

3.1. Resultados preliminares da pesquisa e metodologia

A busca de material na primeira parte da pesquisa foi feita por meio das palavras-chave *segurança*, *cyberespaço*, *cibernética*, *cyberwar*, na biblioteca da PUC-SP. Como já colocado anteriormente, os acervos físicos não possuem muitas obras acerca do tema, portanto uma segunda busca através da Internet foi realizada. As palavras chaves usadas foram *segurança, cibernética, Brasil, Rússia, Xangai e cooperação*. Além das obras encontradas anteriormente – como *Cyber war: the next threat to national security and what to do about it* e *Wired for war: the robotics revolution and conflict in the 21st century*, usei como base os sites do Itamaraty, da Organização de Cooperação de Xangai (disponível em inglês) e do jogo *Global Conflicts*. Ainda por indicação do Prof. Thiago Moreira de Souza Rodrigues, complementei a pesquisa com um relatório sobre a Organização de Cooperação de Xangai feito pelo SIPRI, instituto internacional de pesquisa voltado para conflitos, e o livro *Governança da Internet: aspectos da Formação de um regime global e as oportunidades para a ação diplomática* de Everton Lucero.

Os resultados iniciais da pesquisa estão relacionados a dois dos fluxos em que a pesquisa foi dividida: a procedência do conceito de *cyberwar* e as estruturas burocráticas brasileira e americana voltadas para conflitos dentro do cyberespaço. Em seguida pretendo levantar fontes e analisar primeiramente o Tratado de Não-Agressão por Armas de Informação firmado entre Brasil e Rússia, a Organização de Cooperação de Xangai e os *serious-games*. Ademais, pretendo identificar as crescentes resistências que têm surgido, tanto dentro do Brasil, como o ataque a sites do Governo Federal, quanto outros mais que surgem não só contra Estados.

Os dois livros usados como base foram *Cyber war: the next threat to national security and what to do about it* de Richard Clarke e Robert K. Knake e *Wired for war: the robotics revolution and conflict in the 21st century* de P. W. Singer.

O primeiro apresenta a cyberwar esmiuçando e descrevendo seus componentes. O primeiro capítulo é dedicado aos novos ataques, dando ênfase a um dos primeiro ataques do gênero ocorrido na Síria, próximo à fronteira turca, realizado por Israel, em setembro de 2007. O segundo capítulo trata dos atores dessa nova guerra, primeiro dentro do contexto norte-americano, e em seguida questiona exatamente quem seriam os cyberwarriors e também a vulnerabilidade americana nesse sentido. O terceiro capítulo, chamado "The Battlespace", ou campo de batalha, trata do cyberespaço, visto muitas vezes apenas como a internet; os autores, por outro lado, usam outros exemplos de onde a cyberwar pode acontecer, como por exemplo redes fechadas ou as chamadas "transactional networks".

Os últimos capítulos do livro abordam mais detalhadamente a vulnerabilidade americana diante dessa nova forma de guerra, mostrando que ainda não há estratégia de defesa bem definida dentro da cyber guerra. Por fim, o autor Richard Clarke, que trabalhou no Conselho de Segurança dos Estados Unidos durante o governo de Bill Clinton e parte do governo George Bush, faz algumas sugestões sobre como as novas agendas de segurança relativas à cyber segurança deveriam ser pensadas.

O livro de P. W. Singer, *Wired for war: the robotics revolution and conflict in the 21st century,* apresenta as mudanças ocorridas na forma de se fazer guerra, assim como na 'ética' que envolve a guerra, na política, economia e também nas leis. O livro faz diversos paralelos de tais mudanças com certas tecnologias encontradas na ficção científica. Para mapear o histórico das tecnologias de

guerra, me ative aos capítulos *Introduction: Scenes from a Robot War* e *Smart Bombs, Norma Jeane, and Deafecating Ducks: A Short Story of Robotics.*

Por fim, para melhor entendimento da cyber guerra e para completar a análise crítica acerca do tema, busquei entender o conceito dos novos estados de violência, problematizado por Frédéric Gros. Em *Estados de Violência - Ensaio Sobre o Fim da Guerra,* Gros trata de conflitos pós-modernos e seus novos atores: mercenários, exércitos privados, o crime organizado, etc. Para melhor entendimento, Gros faz um paralelo entre as guerras clássicas e os novos conflitos, expondo seus contrastes e ainda apresenta a o papel da mídia dentro dos estados de violência.

Ainda usando o livro de Gros para embasamento teórico, nessa última parte da pesquisa, realizei o mapeamento das ações da Organização de Cooperação de Xangai e dos acordos referentes à cybersegurança no Brasil. O levantamento de *serious games* também foi realizado, e os desenvolvimentos em ambos foram acompanhados durante esse semestre. Por fim, a descrição e o impacto dos acordos e dos jogos foram explicitados em meu relatório final, e apontados como medidas de cybersegurança.

3.1.a. Procedências do Conceito de Cyberwar

> O avanço tecnológico presenciado nos últimos 30 anos vem acompanhado de novas tentativas de aprimorar a defesa cibernética e a mudança do posicionamento dos países em relação a ela. Atualmente os ataques têm crescido progressivamente e apresentam-se em escala mundial, sendo até mencionados como o grande desafio do século (Clarke e Knake, 2010).

O desenvolvimento de tecnologias também alterou, durante o

século, a forma de se fazer guerra. Modificou estratégias, treinamentos, reportagens de guerra e efetivamente o modo de combate, as armas.

Ao buscar as procedências do conceito de cyberwar, é importante compreender que a maior parte das pesquisas de desenvolvimento de tecnologias que replicam habilidades humanas, sempre estiveram ligadas à guerra. A área na qual tal ligação foi mais explicita, foi na criação das primeiras calculadoras, que precederam os computadores. A primeira calculadora foi inventada em 1820, e foi logo comprada por militares britânicos e franceses, com o intuito de usá-la na trajetória de balas de canhão.

No início do século XX, os avanços já haviam possibilitado com que máquinas pudessem ser controladas à distância, e muito disso se deve a Thomas Edison e Nikola Tesla. As bases para construção de veículos guiados por controle-remoto já eram sólidas no início da Primeira Guerra Mundial, que se mostrou uma mistura de táticas ultrapassadas com tecnologias mais nocivas que as antes utilizadas.

A perda do caráter heróico e a crescente mortalidade da Guerra acabaram por fomentar o interesse por armas não-tripuladas. Em terra, já havia pequenos carros encarregados de levar suprimento às trincheiras, guiado pela luz de lanternas; no ar, a primeira versão dos mísseis guiados como existem hoje O único sistema a ser usado em grande escala, porém, eram barcos alemães que protegiam a costa do país. Estes eram controlados por um piloto na costa, e mais tarde, de um avião que os arrastava. Ambos os sistemas se mostraram pouco eficientes, e em 1916, o controle por rádio, inventado por Tesla, foi incorporado à guerra.

Os alemães, em desvantagem numérica em ambas as guerras, se

mostraram também mais inclinados ao uso de armas não-tripuladas na Segunda Guerra Mundial. A arma mais conhecida se chamava Golias, um pequeno carro que carregava explosivos e era guiado por controle-remoto. No ar também havia inovações, como o míssil de cruzeiro (V-1), o míssil balístico (V-2) e o avião-de-caça (Me-262). Os aliados não possuíam armas tão modernas quanto os alemães, mas incorporaram os mesmos avanços, como o controle por rádio, em suas estratégias.

O avião não-tripulado produzido em maior escala durante a Guerra, por outro lado, foi usado para treinamento e não combate. O OQ-2 Radioplane não gerava muitos custos e era controlado por rádio, serviam de alvos para tornar o treinamento de atiradores mais realista. Após o ataque à Pearl Harbor, o exército passou a comprar o modelo em grandes números e utilizá-lo em combate. Nesse mesmo período outros avanços estavam sendo feitos, dessa vez no campo de sistemas automatizados e computadores.

Em 1920, Carl Norden desenvolveu um computador análogo que podia calcular a trajetória de uma bomba ao cair de um avião em movimento. Em tal situação, a reação humana não seria rápida o suficiente, portanto o sistema lançava bombas automaticamente, em tempo para atingir seu alvo. Ainda que em situações de combate real, o sistema não era tão ágil quanto o esperado, nada tão efetivo como 'o Norden' havia sido criado até então, por esse motivo foi usado em todos os grandes aviões bombardeiros americanos durante a Segunda Guerra. O Projeto Norden custou quase o mesmo que o Projeto Manhattam, que desenvolveu a primeira bomba atômica. A tecnologia foi usada na Segunda Guerra Mundial, nos anos de 1943, 1944 e 1945, e com o fim do conflito, como ainda era considerada inacabada, continuou a ser

desenvolvida e produzida.

Ao fim da Guerra, os aviões que haviam sido equipados com o sistema Norden estavam sendo substituídos por modelos mais sofisticados, como o B-29. O modelo foi o primeiro a ter um sistema de disparo controlado por computador, e foi o mesmo modelo utilizado para lançar a primeira bomba atômica em Hiroshima. O maior avanço, porém, foi aquele dos computadores que não eram usados em campos de batalha, primeiro com o inglês Colossus e em seguida com o primeiro computador eletrônico, o ENIAC. Criado na Pensilvânia, o ENIAC podia calcular equações com rapidez muito maior que qualquer pessoa, e foram inclusive utilizados no desenvolvimento da bomba de hidrogênio no final de 1945. Sua primeira versão comercial foi lançada em 1951.

O avanço tecnológico da robótica e dos computadores seguiu também na Guerra Fria, com os militares como atores centrais. Grace Hopper era uma agente da marinha e participou da criação do primeiro computador digital, o Harvard Mark I, feito pela IBM, em 1944. A agente era parte da equipe que desenvolveu um software capaz de tornar o código de cada máquina em algo universal (Common Business Language), dessa forma os computadores não seriam mais limitados aos cientistas, mas todas as máquinas poderiam se comunicar.

Em 1965, Bob Taylor, cientista da computação e um dos pioneiros da internet, entrou na DARPA (*Defense Advanced Research Projects Agency*), onde desenvolveu um sistema que podia conectar cada computador aos outros em uma rede, e também percebeu que mensagens poderiam ser passadas entre eles com o auxilio de *routers*. Já em 1969, o 'Darpanet' se conectou com sua primeira mensagem a um computador na

Califórnia. Um 'manual de instruções' formal foi criado, em 1973, determinando como diferentes redes poderiam se comunicar com outras. Foi no Protocolo de Controle de Transmição que o termo Internet foi usado pela primeira vez.

Durante todo esse período de avanço nos computadores, a robótica também se expandia e desenvolvia, e em 1976 já estava sendo utilizada nas sondas espaciais Viking 1 e 2. Em 1979, o governo dos Estados Unidos começou a investir no projeto Áquila, que consistia em pequenos mísseis que enviariam informação sobre o número e as intenções dos inimigos em combate, assim como o avião não-tribulado Predador faz hoje em dia. Porém, os altos custos do programa acarretaram em seu cancelamento, em 1987, e o avanço em veículos não-tripulados foi adiado, novamente por preferências políticas e não pela falta de tecnologia em si.

A Guerra do Golfo marca o início da entrada das armas não-tripuladas nas forças estadunidense mesmo que em pequenos números. O destaque dessa operação foi o míssil Pioneer, um avião de segunda-mão comprado de Israel. Em um episódio, soldados iraquianos se renderam ao avistar um Pioneer, foi a primeira vez que soldados se renderam a um sistema não-tripulado. Outro destaque da Guerra foram os mísseis e bombas guiadas, chamadas de '*smart bombs*', geralmente guiadas por lasers. A tecnologia começou a ser desenvolvida pelo exército, mas apenas quando os *microchips* se tornaram suficientemente pequenos, se tornou útil.

Nos Estados Unidos diversas campanhas a favor das armas não-tripuladas foram iniciadas, mesmo estas sendo apenas 7% do armamento usado na Guerra do Golfo. Por outro lado, foi a primeira guerra a ter

computadores como ferramenta tão presente, desde o uso de satélites e previsões das ofensivas iraquianas. Durante a década de 1990, os sistemas se tornaram ainda mais eficazes e em 1995 os sistemas não-tripulados foram integrados a GPS, levando outras forças armadas além da americana a ter interesse na nova tecnologia.

Com a chegada do século XXI, as novas tecnologias evoluíram e se tornaram mais acessíveis, os sistemas não-tripulados mostravam sempre sucesso. Ainda no fim da Guerra Fria, a tolerância da opinião pública quanto a riscos militares mudou radicalmente, a perda de soldados era um ponto extremamente delicado.

Com isso em vista, em 2000, um senador virginiano chamado John Warner, membro importante do *Senate Armed Services Committee*, lançou uma proposta para o Pentágono, na qual um terço de todos os aviões deveriam ser não-tripulados até 2010 e um terço de todos os veículos de combate por terra também, até 2015. Outro forte motivo para a proposta foi a necessidade de encorajar os jovens americanos a se alistarem no exército, as forças armadas acataram a proposta.

Os ataques terroristas de 11 de setembro motivaram as missões militares americanas no mundo e também fomentaram o crescimento do investimento feito nas forças militares, na robótica em particular. De 2002 a 2008 a verba direcionada a defesa subiu em 74%, sem contar as missões já no Iraque e Afeganistão. O principal investimento foi em novas tecnologias, com destaque para as armas não-tripuladas, o incidente é considerado ponto inicial em que as tecnologias não-tripuladas ganharam espaço dentro das forças armadas.

Enquanto 93% das bombas lançadas no Iraque em 1991 eram

"dumb bombs", em 2003 70% delas eram "smart bombs". Com essa mudança no pensamento militar, finalmente se estabelecia a base para a indústria militar robótica, de fato.

Não se pode dizer que tal fenômeno cessará tão cedo por conta de dois motivos: primeiro, essa tecnologia já está avançada o suficiente ao ponto em que 'robôs' são acessíveis e de fato tem alguma utilidade, e segundo, a situação mundial mudou para pior em termos de variedade, sofisticação e letalidade das diversas ameaças agora existentes. Bare Everett, um pesquisador da marinha americana, chega a colocar as novas tecnologias como a 'resposta' aos homens-bomba. (Singer, 2009)

A eficácia dos sistemas não-tripulados, sua precisão e a forma com que eles diminuem drasticamente os riscos em combate tornaram os soldados humanos de certa forma obsoletos. A mentalidade dos militares, especialmente dos americanos, sofreu mudanças drásticas, e já se acredita que a longo prazo, se pode fazer muito mais com essas máquinas, do que sem elas.

O primeiro ataque reconhecido como um cyber ataque, aconteceu na Síria, em 6 de setembro de 2007. Aviões israelenses entraram no espaço aéreo sírio, sem serem detectados, e bombardearam uma construção próxima a fronteira com a Turquia, aonde trabalhavam operários norte-coreanos e segundo o governo israelense, estava relacionada à construção de armas de destruição em massa por parte do governo norte-coreano.

O silêncio político que se seguiu logo após o ataque, mostra o caráter incomum do acontecido. A mídia ocidental, após certo tempo, começou a divulgar o acontecido, e os jornais israelenses eram permitidos

apenas a reproduzir tais noticias. Com certo atraso, o governo sírio admitiu o ataque em seu território, dizendo que a construção era apenas um prédio vazio, e o governo da Coréia do Norte o apoiou.

Se as alegações israelenses fossem verdadeiras, e o governo norte-coreano de fato estivesse de fato envolvido em algum tipo de projeto nuclear, isso significaria a quebra de um acordo feito com os Estados Unidos e outras grandes potências.

Em 2008, a CIA revelou um vídeo clandestino da instalação antes do bombardeio. A evidencia deixou claro que a construção era de fato uma planta nuclear norte-coreana. Pouco tempo depois, a Agencia Internacional de Energia Atômica terminou seu relatório sobre o local, a primeira impressão foi desanimadora pois o local estava completamente vazio, porém amostras do solo revelavam níveis de substancias radioativas 'não-naturais'. Ambas as evidencias provam que, de fato, a Síria estava envolvida com armas nucleares, com ajuda do governo norte-coreano.

Outra particularidade do caso, e a que mais interessa a esta pesquisa, é como os radares sírios de bilhares de dólares falharam ao não prever os ataques israelenses. A força militar israelense havia 'derrubado' o sistema de defesa aéreo sírio, o que chamou a atenção dos russos, de quem o país havia comprado tal tecnologia.

Esta foi a grande primeira demonstração de *cyberwar*, e é como a guerra seria lutada na presente era da informação. Segundo Richard A. Clarke, autor do livro Cyberwar, quando nos referimos a cyberwar, nos referimos a ação de um estado-nação para penetrar em computadores e redes de outras nações, a fim de causar danos.

3.1.b Estrutura burocrática americana

Em resposta aos ataques de onze de setembro, o presidente George W. Bush anunciou a inauguração do Escritório de Segurança Interna, e em novembro de 2002 estabeleceu-se o Departamento de Segurança Interna, com o intuito de reunir todas as organizações ligadas à defesa do Estado num só departamento. O *Department of Homeland Security* (ou Departamento de Segurança Interna) dos Estados Unidos da América que tem como principais responsabilidades proteger o território de ataques terroristas e responder a disastres naturais. Em 2003 o departamento absorveu o Serviço de Imigração e Naturalização e mais pra frente diversos outros órgãos estatais. A primeira controvérsia envolvendo o departamento foi a questão da incorporação, em parte ou totalmente, do FBI e da CIA, que após longa discussão não foram incluídos.

Dentro do departamento existe a *Nacional Cyber Security Division*, que é responsável pelo *Response System*, programa de gerenciamento de riscos, e requisitos para a segurança cibernética nos EUA, dentro da divisão também existem o US-CERT e o *National Cyber Alert System*. Ela coopera com o governo e usuários privados a fazer a transição para as novas capacidades da segurança cibernética e também fundou o Cyber Security Research and Development Center. Em 2009, o Departamento de Segurança Interna inaugurou o *National Cybersecurity and Communication Integration Center*, que comporta organizações governamentais responsáveis por proteger redes de computadores e infra-estruturas em rede.

O departamento tem sido fortemente criticado pela opinião pública por representar um excesso burocrático, um desperdício e ineficácia. O congresso estima que tenha gastado 15 bilhões de dólares em contratos falidos e já foram

registrados casos de fraude e corrupção. O departamento surgiu como instrumento da 'guerra ao terror', porém não realizou descobertas significativas a respeito de possíveis ameaças terroristas dentro do país, e se mostra um tanto inútil frente às poucas ameaças sofridas desde 2001, ou ao menos, a um número menor do qual se cogitava.

Em 16 de maio de 2011, a Casa Branca lançou a primeira agenda de segurança voltada para o *cyberespaço*. A agenda pretende apresentar ao público e à comunidade internacional qual a posição dos Estados Unidos sobre o *cyberespaço*. As principais metas definidas no documento são a construção de prosperidade, o aprimoramento da segurança e a aproximação de outros Estados para que essas metas sejam atingidas (http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace).

A primeira consideração do governo americano consiste na segurança cibernética, vista como uma obrigação dos Estados e das sociedades e não um fim em si mesmo. O principal objetivo dessa nova forma de segurança é que a inovação tecnológica continue acontecendo, tanto para o desenvolvimento de mercados, quanto para a vida das populações. Três princípios são estabelecidos, que já são conhecidos entre as políticas americanas: a liberdade de expressão, a privacidade e a livre circulação de informação.

A agenda americana alega que infra-estruturas digitais são o respaldo de economias prósperas, comunidades de pesquisa, forças militares fortes e sociedades livres. Como já visto, tais estruturas também são responsáveis pela distribuição de água, eletricidade, o controle de vôos e o suporte do sistema financeiro, ou seja, estruturas críticas de todos os países. Para que essas tecnologias continuem a beneficiar indivíduos, sociedades, pesquisas,

desenvolvimento e as inovações necessárias para a construção de economias modernas, a grande abertura e cooperação existentes, que já as caracterizam devem ser preservadas, porém no plano de estratégia americano, fica claro que essas redes devem ser confiáveis e seguras (INTERNATIONAL STRATEGY FOR CYBERSPACE – Prosperity, Security, and Openness in a Networkes World, pág. 3).

Um dos pontos mais recorrentes no documento, é que o reconhecimento dos desafios instituídos por "atores mal-intencionados" deve ser feito coletivamente, e que deve haver uma atualização de políticas nacionais e internacionais, para que essas sejam fortalecidas dentro do *cyberespaço*. Além desses desafios, alguns outros exemplos são usados, como desastres naturais, problemas técnicos e até roubo de propriedade intelectual. A fundação das novas políticas americanas, consiste, segundo tal agenda, na crença de que as redes existentes são de grande potencial para os Estados Unidos e para o mundo.

O governo americano estabelece que irá confrontar os novos desafios, preservando os princípios básicos já estabelecidos. O país se compromete com iniciativas internacionais que desenvolvam a segurança cibernética, reconhecendo assim suas responsabilidades globais e seus interesses nacionais. Muitas vezes, os princípios que baseiam a forma de ação americana são incompatíveis com o "uso de lei efetivo" (INTERNATIONAL STRATEGY FOR CYBERSPACE – Prosperity, Security, and Openness in a Networkes World, pág. 5), porém a nova agenda de estratégia americana tenta mostrar como boas políticas de segurança cibernética podem aprimorar a privacidade, o uso efetivo de leis e as liberdades fundamentais.

É apresentado um objetivo referente ao futuro do *cyberespaço,* que

pretende promover uma infraestrutura aberta, inter-operacional, segura e confiável de informações e comunicações, que apóie a troca, o comércio, a segurança internacional e fomente a expressão e inovação livre. Para tanto, o governo americano pretende construir e sustentar um ambiente em que "normas de comportamento responsável" guiem os Estados e suas ações, sustentando parceirias e apoiando a lei dentro do *cyberespaço (*INTERNATIONAL STRATEGY FOR CYBERSPACE – Prosperity, Security, and Openness in a Networkes World, pág. 8). Outros princípios colocados como "a base das normas" para a cybersegurança são: sustentação das liberdades fundamentais, respeito pela propriedade, apreço pela privacidade, proteção contra o crime e direito de autodefesa pelos Estados; outros princípios não tão tradicionais também são listados, como colaboração global, estabilidade de redes, acesso confiável, governança global perante os desafios da Internet e a responsabilidade de cada estado para proteger seu *cyberespaço.*

O governo americano também determina seu papel no futuro do cyberespaço, combinando diplomacia, defesa e desenvolvimento para atingir prosperidade, segurança e abertura para que todos possam se beneficiar das tecnologias. Seu objetivo diplomático é trabalhar para criar incentivos para um ambiente internacional no qual Estados trabalhem juntos e atuem com responsabilidade (INTERNATIONAL STRATEGY FOR CYBERSPACE – Prosperity, Security, and Openness in a Networkes World, pág. 11). Já no quesito defesa, os Estados Unidos pretendem defender suas redes, independente se a ameaça venha de "terroristas, criminosos cibernéticos ou outros Estados". O objetivo, nesse caso, fica estabelecido como uma parceria com outros Estados para encorajar um "comportamento responsável" contrário aos que pretendem corromper as redes e sistemas, e reservando o direito de defender essas propriedades nacionais vitais de forma necessária e apropriada.

Por fim, estabelecem o objetivo referente ao desenvolvimento, e prometem facilitar a capacidade de produção de *cybersegurança,* por organizações multilaterais e bilaterais, para que cada país tenha a capacidade de proteger suas estruturas digitais, fortalecer as redes globais e construir parcerias mais fortes (INTERNATIONAL STRATEGY FOR CYBERSPACE – Prosperity, Security, and Openness in a Networkes World, pág. 14)

3.1.c. Estruturas burocráticas brasileiras

Segundo o Conselho de Segurança Nacional russo, o Brasil faz parte dos 16 países capazes de se valer de ataques cibernéticos e já é estimado que, no país, há cerca de 2000 ataques a grandes redes do governo por hora, com a finalidade de roubar dados e informações. Portanto, a segurança cibernética já é tida como função estratégica do Estado.

O Governo brasileiro ainda vai mais longe no desenvolvimento da segurança cibernética, já tem um Curso de Especialização em Gestão da Segurança da Informação e Comunicação na UnB e tinha planos de modelar novo curso de mestrado na mesma área. Ao consultar o site da UNB e do CEGSIC, Curso de Especialização em Gestão da Segurança da Informação e Comunicações, encontrei apenas o curso já vigente.

O curso de Especialização em Gestão da Segurança da Informação e Comunicação oferece formação necessária para desenvolver tecnologias, projetos e softwares, implantar, operar e gerneciar redes de telefonia, televisão e comunicações de dados. Também produzir conteúdo e aplicações multimídia para integrar todos os serviços de redes.

Dentro do mercado de trabalho, o profissional pode exercer atividades como engenheiro projetista de redes, integrador de sistemas de comunicação,

de desenvolvimento de sistemas distribuídos, de instalação e operação de redes, gerente de redes, administrador de áreas de teleinformática, planejador de arquiteturas corporativas de tecnologia da informação, acessor técnico, engeneiro técnico-comercial, consultor independente, gestor da segurança da informação, entre outros cargos. Basicamente a formação permite atuação em todos os ambientes de aplicação das redes de comunicação.

Segundo a UnB, cursos do gênero são de enorme importância no Brasil, já que a utilização dos serviços de redes aumenta exponencialmente e abrangem a maior parte das atividades sociais e todos os setores econômicos (http://dsic.planalto.gov.br/cegsic).

Também existem tratados e programas internacionais relativos ao debate, e já se aproxima um fortalecimento em nível nacional e internacional de cooperação técnica, por exemplo, o tratado firmado entre Brasil e Rússia, em 2010, chamado de "Acordo de Não Agressão por Armas de Informação" que estabelece trocas de informação usadas na capacitação de pessoal e a realização de ações conjuntas de guerra cibernética. Este acordo é um dos pioneiros da área, só existindo semelhante o Acordo de Cooperação de Xangai.

Em paralelo à estrutura burocrática e o INTERNATIONAL STRATEGY FOR CYBERSPACE – Prosperity, Security, and Openness in a Networkes World, publicado pelos Estados Unidos, o Brasil possui o Comitê Gestor da Internet, criado em 1995 e constituído pelo Ministério das Comunicações e o Ministério da Ciência e Tecnologia. O Comitê foi visto como necessário, pois apenas dessa forma haveria efetiva participação da sociedade em ações para a implantação, administração e uso da Internet, e fazem parte dele o Ministério das Comunicações e o Ministério da Ciência e Tecnologia, entidades operadoras e gestoras de espinhas dorsais, representantes de provedores de acesso ou de

informações, representantes de usuários, e a comunidade acadêmica (http://www.cgi.br/) O CGI aprovou uma resolução, durante sua 3ª reunião em 2009, que aprovou 10 Princípios para a Internet no Brasil, os princípios seguem anexados ao Relatório Final.

3.1.d) A Organização de Cooperação de Xangai

A Organização representa o sucesso do protótipo *Shangai Five,* e se trata de uma organização internacional formada por China, Quirguistão, Rússia, Tadjiquistão e Uzbequistão, desde junho de 2011.

Os principais objetivos da Organização são fortalecer a confiança e boa relação entre seus países membros, promovendo cooperação política, econômica e de trocas, de ciência e tecnologia, cultura, educação, energia, transportes, turismo, ecologia, e muitos outros campos, chegando a abranger a cybersegurança.

A Organização de Cooperação de Xangai é primariamente centrada em seus membros, todos nações do centro-asiático com preocupações de segurança em comum, as ameaças mais comuns são o terrorismo, o separatismo e o extremismo, porém suas ações na área de desenvolvimento social tem crescido progressivamente. Em 2004, a Estrutura Anti-terrorismo Regional foi inaugurada, e em 2006 foram anunciados planos contra as infrações relativas ao tráfico de drogas ilícitas nas regiões de fronteira, e também foi declarado que a organização não tem planos de se tornar um bloco militar. Já em 2007 foi firmado um contrato com a Collective Security Treaty Organisation, aliança militar intergovernamental formada por Estados centro-asiáticos, para ampliar as cooperações relacionadas ao trafico de drogas, segurança e o crime.

A organização também está redefinindo o cyberwarfare (ações de um Estado-nação para penetrar em computadores de outros com o propósito de causar dano), dizendo que a disseminação de informações "nocivas as esferas espirituais, morais e culturais de outros Estados" deve ser considerada uma ameaça a ordem internacional. Um acordo firmado em 2009 definiu o termo "guerra de informação", como uma tentativa de minar os sistemas políticos, econômicos e sociais de outros Estados.

Nos últimos anos, as atividades da organização se expandiram para incluir cooperação militar avançada, compartilhamento de inteligência e contra-terrorismo, oficiais russos iniciaram um dialogo sobre a entrada da Índia no grupo e o possível início de uma aliança militar. No âmbito econômico, todos os membros, salvo a China, também fazem parte da Eurasian Economic Community e com o intuito de aprimorar a cooperação econômica, todos os membros também assinaram um acordo em 2003, e na mesma reunião, Wen Jiabao, 6º premiê chinês, propôs, a longo prazo, o estabelecimento de uma zona de livre comércio na região, enquanto medidas imediatas seriam tomadas para melhorar o fluxo de bens. Por fim, também há cooperação cultural dentro da organização, ministros da cultura dos membros se encontraram pela primeira vez na China para firmar um acordo de cooperação contínua, e festivais de arte e exibições já aconteceram, assim como de dança folclórica.

3.1.e) Acordo de não-agressão por armas de informação e o Brasil frente à questão da segurança cibernética

Tendo em conta as novas ameaças a redes de dados, informações e propriedade intelectual, Brasil e Rússia firmaram, em 2012, um acordo de ajuda mútua a fim de evitar e reagir a ataques cibernéticos. O acordo chamado de Acordo de Não-Agressão por Armas de Informação não está disponibilizado no site do Itamaraty de forma clara, existem apenas diversos acordos acerca do tema que foram firmados durante a reunião de maio de 2010. Contudo, a informação disponível é suficiente para entender os esforços conjuntos entre os dois países, provenientes da preocupação com a cybersegurança.

A série de resoluções prevê trocas de informações para capacitação de pessoal, realização de exercícios conjuntos de guerra cibernética e visa a cooperação para o lançamento de satélites e a construção de foguetes e aviões.

O acordo é um dos primeiros de seu gênero no mundo, assim como o acordo entre os membros da Organização de Cooperação de Xangai. A iniciativa partiu da Rússia e pretende ser ampliado, o Conselho de Defesa Nacional russo indentificou dezesseis países capazes de se valer de ataques cibernéticos, ou como chamaram, ataques de informação, entre eles está o Brasil.

Dentro do acordo, explicitarei apenas alguns projetos mais pertinentes à pesquisa, que serão posteriormente anexados em seu todo a este relatório. O primeiro projeto a ser levado em conta é o de Informação Científico-Tecnológica, que pretende fazer um intercâmbio de informações técnico-científicas por meio de uma base de dados. Os interlocutores russos são o Instituto Nacional de Informação Científica e Tecnológica da Academia de Ciências da Rússia e o Centro de Informação Técnico-científica da Federação Russa; enquanto o brasileiro, o Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT).

Em segundo lugar, há o projeto de nanotecnologia, que nesse primeiro momento visa apenas desenvolver tecnologias médicas como implantes, porém já está relacionada a instituições militares. O projeto é em parceiria com o Instituto de Física de Materiais Avançados da Universidade Estatal Técnica de Aviação, Instituto de Metalurgia e Materiais A. A. Baykov da Academia de Ciências da Rússia e com a Associação Brasileira da Indústria de Artigos e Equipamentos Médicos, Odontológicos, Hospitalares e de Laboratórios, o INMETRO, a Universidade Federal do Rio de Janeiro e o Laboratório de Biomateriais do Instituto Militar de Engenharia. Outras três pesquisas conjuntas de nanotecnologia, com diferentes objetivos, estão em curso, porém não serão citadas especificamente na pesquisa por não possuirem relação com instituições militares.

Por fim, foram firmados dois acordos referentes a Tecnologias da Informação e das Comunicações, sendo o primeiro referente à segurança da informação, e o segundo ao desenvolvimento de algoritimos e redes neurais e computadores neurais, ou seja, que reproduzem a função dos neurônios, tendo menor velocidade, mas realizando diversos processos simultaneamente, para as áreas de alta tecnologia, ciência e medicina. O primeiro, destes dois acordos, representa a preocupação do Brasil frente aos conflitos cibernéticos. E pretende unir esforços de ambas as partes para enfrentar as ameaças à segurança internacional da informação e da comunicação e assegurar os interesses de Brasil e Rússia referentes à cybersegurança. Os interlocutores deste último projeto são Centro Internacional de Informática e Eletrônica (russo), o Parque Tecnológico Capital Digital (Governo do Distrito Federal) e Núcleo de Tecnologia da Informação (NTI) da Universidade de Brasília (UnB).

Os acordos firmados entre Brasil e Rússia que foram considerados relevantes a pesquisa após mapeamento de documentos sobre o tema e firmados na ocasião do Acordo de Não-Agressão por Armas de Informação estão anexados a este relatório final.

3.1.f) *Serious Games*

A criação dos *video games* sempre esteve ligada à guerra. William Higinbotham, cientista nuclear que participou da criação da primeira bomba

atômica, criou o primeiro jogo eletrônico: o tênis para dois. Posteriormente, Steve Russel, inspirado pela corrida espacial e a popularização das histórias em quadrinho, criou o *Spacewar!*, em 1961, primeiro jogo para o único computador do período, o PDP-1.

Os conflitos da guerra fria, da Coréia a Berlim, passaram a ser televisionados. A televisão tornou-se um instrumento para documentar o combate, mas não para interferir naquelas cenas. O sentimento das guerras foi aproximado daqueles que não estavam envolvidos, que por sua vez, não podiam interferir nas imagens que viam.

Em 1972, Nolan Bushnell criou o Atari, que foi o marco do início da indústria de jogos eletrônicos. O desenvolvimento dos jogos sempre buscou aproximá-los da realidade, desde suas imagens até mecanismos para que os jogadores se sentissem dentro da situação em que o jogo acontecia.

Os *serious games* combinam a realidade de guerra, mostrada detalhadamente nos jogos, com o poder de interferência. Os jogos em questão na pesquisa são os jogos de recrutamento, como por exemplo o America's Army, um simulador de guerra criado e usado pelo exército americano, ou o Flight Simulator usado pela aeronáutica americana. Na primeira fase do jogo America's Army é necessário fazer um treinamento básico para que se seja aprovado, com a evolução do jogo e o número de inimigos mortos, o jogador

recebe ‘pontos de honra’ e também é possível atender a uma série de ‘cursos de especialização’ dentro do exército americano. O jogo apresenta um novo grau de realismo e cooperativismo entre os que o jogam, o termo ‘cidadão soldado’ é usado nesses jogos de realidade de guerra.

As novas tecnologias e a assimilação desses novos jogos de estratégia de guerra fomentou o surgimento de um novo modelo de treinamento militar em que os soldados simulam os combates sem riscos físicos e também atingiu os civis, que não teriam contato com experiências de combate, ainda que circunscrito pelo plano da virtualidade.

Na presente pesquisa, o jogo Global Conflicts e sua verão brasileira Conflitos Globais serão objetos de estudo. Global Conflicts é considerado um jogo educacional, com o objetivo de ensinar cidadania, geografia e cursos de mídia. O jogo permite que estudantes aprendam sobre conflitos ao redor do mundo ao inseri-los nos mesmos. Temas como democracia, direitos humanos, globalização, terrorismo, mudanças climáticas e pobreza são os mais abordados.

Os jogos são desenvolvidos para que tenham fácil aplicação na grade curricular de cada país em que são utilizados e sua função seria de aplicação direta em salas de aula, e dessa forma, facilitar a aprendizagem acerca dos temas apresentados.

Em seu vídeo de apresentação (disponível no site http://www.globalconflicts.eu/), mostram a importância dos jogos, visto que o público ao qual é destinado não tem contato direto com conflitos globais ou a pobreza existente no mundo, e nos jogos, tem de desempenhar a função de um jornalista colocado a frente de conflitos éticos. Também é colocada a importância desse tipo de abordagem educacional, visto que os jogos são uma ligação direta ao que se ensina teoricamente e a prática. Ao mesmo tempo aumentam a motivação e personalizam o aprendizado, visto que os alunos têm diferentes possibilidades dentro dos embates éticos que lhe são apresentados. No site do jogo estão disponíveis guias para os professores e tarefas já definidas para os alunos.

O jogo tem diversas versões: o ataque à uma escola no Afeganistão, conflitos em fronteiras israelitas, a procura de um terrorista palestino, o trabalho infantil em Bangladesh, as crianças-soldado em Uganda, a imigração mexicana para os Estados Unidos, os conflitos em fazendas bolivianas e a violência na Guatemala.

O jogo foi traziado ao Brasil, em sua versão Conflitos Globais, pelo professor Gilson Schwartz da ECA-USP, atuante na criação de ambientes educacionais em novas mídias e na articulação entre escolas, mercados, universidades e o governo. A versão nacional foi a primeira iniciativa brasileira

no evento Games for Change, realizado na Parsons School of Desing. O jogo foi criado em parceiria com a empresa SGI, da Dinamarca, com o objetivo de promover práticas pedagógicas distintas nas escolas brasileiras e mantendo o mesmo princípio do jogo Global Conflicts.

Dessa forma, é possível observar as grandes duas funções dos novos *serious games*, eles aproximam a população civil com os conflitos e guerras, tanto para fins de recrutamento como para melhor entendimento dos mesmos. Ambos são fins problemáticos, visto que a guerra como era lutada anteriormente, já não é mais a mesma, jovens são recrutados de dentro de suas casas para atuar na guerra à distância. A relação entre os soldados e a guerra em si foi drásticamente alterada. Além disso, os "princípios" e valores ensinados por jogos como o Global Conflicts são por vezes muito subjetivos, e podem ser vistos como uma imposição aos alunos ainda na escola.

Toda a tragetória das tecnologias de guerra, em conjunto com as novas formas de conflito, deu margem para que os crimes cibernéticos surgissem. Com eles aparece a necessidade de uma agenda de segurança internacional, a fim de estabelecer e institucionalizar uma governança da Internet.

A democratização da informação, e consequentemente do acesso à Internet dificulta questões como a aplicação de leis, combate a criminalidade, as relações comerciais, as regras da propriedade intelectual, as doutrinas de defesa

nacional contra ataques cibernéticos e a institucionalidade da governança global, vista que a governança da Internet tem de ser tratada de forma distinta (Lucero, 2004).

O desenvolvimento de um regime global para a Internet pede a articulação de diferentes atores, e cabe à diplomacia pensar dentro do regime existente, qual a melhor alternativa para que seu funcionamento atenda às novas ameaças. No Brasil, o CGI é um modelo de gestão de recursos da rede, já que envolve o setor privado, acadêmico, governamental e não-governamental. Tal estrutura confere legitimidade e substância à ação externa brasileira referente ao tema (Lucero, 2004).

A própria natureza dos governos e da soberania está sendo alterada pela revolução da informação, e o *soft power* está se tornando cada vez mais importante para as políticas externas, assim como grupos não-governamentais (Nye, 2002). Individuos e instituições privadas ganham cada vez mais espaço na discussão acerca da formulação de políticas externas e políticas de defesa.

3.2. Anexo 1

Resoluções

Resolução CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL

O Comitê Gestor da Internet no Brasil – CGI.br, reunido em sua 3ª reunião ordinária de 2009 na sede do NIC.br na Cidade de São Paulo/SP, decide aprovar a seguinte Resolução:

CGI.br/RES/2009/003/P - **PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL**

Considerando a necessidade de embasar e orientar suas ações e decisões, segundo princípios fundamentais, o CGI.br resolve aprovar os seguintes Princípios para a Internet no Brasil:

1. Liberdade, privacidade e direitos humanos

O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

2. Governança democrática e colaborativa

A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.

3. Universalidade

O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.

4. Diversidade

A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.

5. Inovação

A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.

6. Neutralidade da rede

Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.

7. Inimputabilidade da rede

O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da

liberdade, da privacidade e do respeito aos direitos humanos.

8.Funcionalidade, segurança e estabilidade

A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

9. Padronização e interoperabilidade

A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.

10. Ambiente legal e regulatório

O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração

3.2. Anexo 2: Compilação de programa e acordos assinados entre Brasil e Rússia em 14 de maio de 2010. (disponível em http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/atos-assinados-por-ocasiao-da-visita-do-presidente-luiz-inacio-lula-da-silva-a-russia-2013-14-de-maio-de-2010/?searchterm=tratado%20russia%20brasil)

PROGRAMA DE COOPERAÇÃO CIENTÍFICO-TECNOLÓGICA ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DA FEDERAÇÃO DA RÚSSIA PARA O PERÍODO DE 2010 A 2012

O presente Programa foi preparado conforme a decisão da V Reunião da Comissão Intergovernamental Brasil-Rússia para a Cooperação Econômica, Comercial, Técnica e Científica, realizada em 17 e 18 de novembro de 2008, em Brasília.

O Programa:

- considera os interesses e prioridades de ambas as Partes nas áreas científica, tecnológica e de inovação;

- visa ampliar e intensificar a cooperação das Partes no desenvolvimento e implementação de novas tecnologias, na realização de pesquisas científicas e na formação de profissionais em ciência;

- considera a experiência acumulada pelas Partes durante a implementação dos programas anteriores em áreas como astronomia, optoeletrônica, utilização de gás natural em meios de transporte e metrologia.

As Partes partem do princípio de que os projetos incluídos no Programa contribuirão para o cumprimento de objetivos sociais como o aumento do nível de emprego e de renda, a melhoria do sistema de saúde e da qualidade de educação.

As Partes chegaram ao entendimento sobre a necessidade de seguir aprimorando os mecanismos de implementação de projetos que formam a base

do presente Programa, com vistas a incrementar a cooperação entre o Brasil e a Rússia nas áreas da ciência, tecnologia e inovação.

Este Programa inclui 29 (vinte e nove) projetos de cooperação, mutuamente acordados, que terão avaliação periódica dos resultados, em reuniões com representantes dos dois países. Para efeitos da implementação dos 29 projetos e programas listados abaixo, receberão atenção inicial os projetos 1, 2, 19, e 24.

As Partes envidarão esforços para facilitar e assegurar contatos bilaterais necessários entre as correspondentes entidades de pesquisa científica do Brasil e da Rússia, com o fim de elaborarem projetos nas 29 áreas.

	Nº	**Projeto**	**Interlocutor Russo**	**Interlocutor Brasileiro**
Informação Científico-Tecnológica	1	Intercâmbio de informação técnico-científica em várias formas, acumulada em bases de dados	Instituto Nacional de Informação Científica e Tecnológica da Academia de Ciências da Rússia e Centro de Informação Técnico-científica da Federação da Rússia	Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) -
Metrologia	2	Realização de projetos no âmbito do Memorando de entendimento sobre cooperação técnico-científica na área da metrologia	Agência Federal de Regulamentação Técnica e de Metrologia	Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO

Biologia	3	Utilização de métodos fluorescentes modernos para biomonitoramento ecológico de organismos de fitoplâncton em águas abertas do Brasil	Universidade Estatal de Moscou Lomonosov	Sociedade Brasileira de Biofísica (SBBf)
Matemática	4	Ondas de combustão em meios porosos	Instituto de Mecânica da Universidade Estatal de Moscou Lomonosov	Instituto Nacional de Matemática Pura e Aplicada (IMPA)
Nanotecnologia	5	Elaboração de ligas nanoestruturadas de titanio para implantes e equipamentos médicos	Instituto de Física de Materiais Avançados da Universidade Estatal Técnica de Aviação (Ufa); Instituto de Metalurgia e Materiais A. A. Baykov da Academia de Ciências da Rússia	Associação Brasileira da Indústria de Artigos e Equipamentos Médicos, Odontológicos, Hospitalares e de Laboratórios (ABIMO); INMETRO; Universidade Federal do Rio de Janeiro (UFRJ); Instituto Militar de Engenharia – Laboratório de Biomateriais

Nanotecnologia	6	Materiais Nanoestruturados: aspectos científicos básicos e técnicos e aplicações	Universidade Estatal de Moscou Lomonosov	Universidade Federal do Estado de Pernambuco (UFPE) e INMETRO
	7	Elaboração de policristais sintéticos à base de diamante e nitreto de boro cúbico, modificados com adições em nano-dispersão	Instituto Estatal de Aço e Ligas (Moscou) – Laboratório de Processos de Altas Temperaturas, Materiais e Diamantes	Universidade Federal do Rio Grande do Sul (UFRGS) – Instituto de Física
	8	Estudo de efeitos e superfícies de separação e características físico-mecânicas de nanomateriais	Instituto de Problemas de Química Física (Chernogolovka) da Academia de Ciências da Rússia	Universidade Federal do Rio Grande do Sul (UFRGS) – Instituto de Física
	9	Nanomateriais de volume com três modos: 1) consolidação de nano-pó; 2) nano-cristalização de materiais amorfos de volume; 3) deformação plástica intensiva	Instituto de Física de Materiais Avançados da Universidade Estatal Técnica de Aviação (Ufa) Instituto de Metalurgia e Materiais A.A.Baykov	Universidade Estadual de Maringá Universidade Federal de São Carlos (UFSCAR) - Laboratório de Metais Amorfos e Nanocristalino

			da Academia de Ciências da Rússia	s
	10	Magnetorresistência Gigante de Injeção	Universidade Politécnico de São Petersburgo, Centro de Pesquisas Avançadas	Universidade Federal do Rio Grande do Sul (UFRGS)
	11	Transições de fase de materiais induzidas por choque ; Propriedades termodinâmicas de materiais a altas pressões e temperaturas; Propriedades mecânicas de materiais sob grande tensão aplicada	Instituto de Física de Altas Pressões da Academia de Ciências da Rússia (Troitsk)	Universidade Federal do Rio Grande do Sul (UFRGS) – Instituto de Física
Nanotecnologia	12	Modificação de propriedades de poliolefinas (polipropileno) pela incorporação de nanotubos de carbono; Desenvolvimento de	Instituto de Química Física N.N.Semenov da Academia de Ciências da Rússia	Universidade Federal do Rio Grande do Sul (UFRGS) – Escola de Engenharia e Universidade Federal de Minas Gerais (UFMG)–

		compósitos polipropileno-nanotubos de carbono; Síntese de novos nanocompósitos avançados de polímeros		Instituto de Física
Meio Ambiente	13	Análise dos efeitos do clima nas características da matéria orgânica e substâncias húmidas do solo	Universidade Estatal de São Petersburgo – Faculdade de Biologia e Solo	EMBRAPA
Biotecnologia	14	Biotecnologia para produção de biogás e energia a partir de resíduos da agroindústria	Instituto de Microbiologia da Academia de Ciências da Rússia	EMBRAPA
	15	Desenvolvimento de marcadores moleculares associados à qualidade de carne bovina	Instituto de Pesquisa Genética e Criação de Animais da Academia de Ciências Agrícolas da Rússia (São-Petersburgo-Puchkin)	EMBRAPA
	16	Sistemas geoinformáticos para optimização do uso de fertilizantes minerais em	Universidade Estatal de Moscou Lomonosov	EMBRAPA, Centro Nacional de Pesquisa de Solos

		agricultura		
	17	Tecnologia de Produção de Alimentos – Carne Suína	Instituto de Pesquisa da Indústria de Carnes da Academia de Ciências Agrícolas da Rússia	EMBRAPA
Saúde	18	Influência de venenos de cobras, aranhas, escorpiões e outros animais peçonhentos sobre o sistema nervoso periférico	Instituto de Química Bio-orgânica N.N.Shemyakin-I.A.Ovchinnikov	Instituto Butantan
	19	Rede de Cooperação Tecnológica HIV/AIDS – Construção de 3 painéis – sorológico, imunológico e de genotipagem	Instituto de Química Bio-orgânica N.N.Shemyakin-I.A.Ovchinnikov	Instituto Butantan
	20	Controle Neuro-Endócrino do Desenvolvimento de Triatomídeos	Universidade de Amizade dos Povos (Moscou) - Instituto de Pesquisa de Desinfectologia	Fundação Oswaldo Cruz (FIOCRUZ)
	21	Espécies de *Eugenia murtaceae* como Agentes Antidiabéticos Naturais	Universidade de Amizade dos Povos (Moscou) - Universidade Estatal Instituto de Pesquisa de Plantas Medicinais e Aromáticas	Fundação Oswaldo Cruz (FIOCRUZ)
	22	Pesquisa de Agentes	Universidade de	Fundação

		Naturais para Tratamento de Tuberculose	Amizade dos Povos (Moscou) - Instituto de Pesquisa de Epidemiologia e Microbiologia (Vladivostok) da Academia de Ciências da Rússia	Oswaldo Cruz (FIOCRUZ)
Física	23	Estabilidade e oscilações de sistemas mecânicos não-lineares	Instituto de Mecânica da Universidade Estatal de Moscou Lomonosov	Universidade Estadual Paulista (UNESP)
	24	Pesquisa de interações hiperfinas em intermetálicos por correlações angulares de gama-quantos	Instituto de Pesquisa de Física Nuclear da Universidade Estatal de Moscou Lomonosov	Centro Brasileiro de Pesquisas Físicas (CBPF)

Física	25	Pesquisas dinâmicas dos satélites naturais do sistema solar	Instituto de Astronomia Aplicada da Academia de Ciências da Rússia	Observatório Nacional
	26	Energia escura,	Cento de	Centro

		matéria escura, e objetos compactos de alta densidade no Universo: modelos multidimensionais de gravitação, cosmologia e evidências astronômicas	Gravitação e Metrologia Fundamental (VNIIMS) e Instituto de Gravitação e Cosmologia da Universidade de Amizade dos Povos (Moscou)	Brasileiro de Pesquisas Físicas (CBPF)
	27	Desenvolvimento da teoria das interações fundamentais com possibilidade de verificação na física de partículas elementares e na cosmologia	Universidade Pedagógica Estatal de Tomsk	Universidade Estadual de Londrina – Departamento de Física
Tecnologias da Informação e das Comunicações (TICs)	28	Segurança da Informação	Centro Internacional de Informática e Eletrônica	Parque Tecnológico Capital Digital (Governo do Distrito Federal) e Núcleo de Tecnologia da Informação (NTI) da Universidade de Brasília (UnB)
	29	Desenvolvimento dos algoritmos e redes neurais e computadores	Centro Internacional de Informática e Eletrônica	Universidade Federal do Rio de Janeiro

		neurais para as áreas de alta tecnologia, ciência e medicina		Núcleo de Atendimento de Computação de Alto Desempenho (NACAD-COPPE/UFRJ)

Novas formas da Cooperação em Ciência e Tecnologia

As Partes reafirmam a necessidade de ampliar as formas de cooperação bilateral e realizar mais sistematicamente seminários e conferências científicos e preparar programas de trabalho em áreas de ciência, tecnologia e inovação. As Partes manifestaram a disposição de estabelecer o intercâmbio regular da informação de caráter científico-tecnológico, organizar a formação conjunta de profissionais em ciência e promover o desenvolvimento de estágios de cientistas em centros de pesquisa e laboratórios de referência nos dois países. No primeiro semestre de 2010, as Partes discutirão em contatos bilaterais a possibilidade de criação de centros bilaterais de inovação.

O presente Programa poderá ser ampliado e ajustado com o consentimento das Partes.

O presente Programa não é tratado internacional, não contém direitos e obrigações regularizados pelo direito internacional.

Feito em Moscou, em 14 de maio de 2010, em dois originais, em português e russo.

*****

ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DA FEDERAÇÃO DA RÚSSIA SOBRE A PROTEÇÃO MÚTUA DA PROPRIEDADE INTELECTUAL E OUTROS RESULTADOS DA ATIVIDADE INTELECTUAL UTILIZADOS E OBTIDOS NO CURSO DA COOPERAÇÃO TÉCNICO-MILITAR BILATERAL

O Governo da República Federativa do Brasil

e

O Governo da Federação da Rússia,

doravante denominados as Partes,

Em conformidade com os termos do Tratado sobre Ações de Parceira entre a República Federativa do Brasil e a Federação da Rússia, assinado em Moscou, em 22 de junho de 2000,

Orientados pelo Memorando entre o Governo da República Federativa do Brasil e o Governo da Federação da Rússia sobre Cooperação no Domínio de Tecnologias Militares de Interesse Mútuo, assinado em Moscou, no dia 9 de abril de 2002,

Tendo em conta o Acordo entre o Governo da República Federativa do Brasil e o Governo da Federação da Rússia sobre Cooperação Técnico-Militar, assinado no Rio de Janeiro, no dia 26 de novembro de 2008,

Reafirmando a intenção das Partes de fortalecer os laços de amizade entre os dois Estados,

Reafirmando os direitos e as obrigações no âmbito dos acordos internacionais dos quais a República Federativa do Brasil e a Federação da Rússia são partes,

Reconhecendo a importância da proteção mútua da propriedade intelectual e de outros resultados da atividade intelectual usados e obtidos no curso da cooperação técnico-militar bilateral,

Tendo em consideração a necessidade de coordenar os esforços das Partes e de assegurar medidas efetivas para prevenir e reprimir quaisquer violações relacionadas à propriedade intelectual e a outros resultados da atividade intelectual usados e obtidos no curso da cooperação técnico-militar,

Aderindo aos princípios da igualdade e dos benefícios mútuos, acordaram o que segue:

Artigo 1

O propósito do presente Acordo será prever as condições para proteção legal da propriedade intelectual e de outros resultados da atividade intelectual usados e obtidos exclusivamente no curso da cooperação técnico-militar bilateral, em conformidade com a legislação da República Federativa do Brasil ou a legislação da Federação da Rússia, respectivamente, e com os tratados internacionais dos quais a República Federativa do Brasil e a Federação da Rússia são partes.

Artigo 2

Para fins do presente Acordo, os seguintes termos serão utilizados:

"cooperação técnico-militar"- atividades no campo das relações internacionais relacionados à exportação e à importação, inclusive oferta ou compra, de

produtos com finalidades militares, bem como ao seu desenvolvimento, fabricação e modernização;

"produtos para fins militares"- armamento, material, bem como trabalhos (incluindo desenvolvimentos tecnológicos e outros), serviços (incluindo apoio logístico, treinamento profissional e outros), propriedade intelectual e outros resultados da atividade intelectual e informação pertinentes à esfera técnico-militar;

"propriedade intelectual"- interpretada pelo presente Acordo conforme estabelecido no Artigo 2 da Convenção que estabelece a Organização Mundial de Propriedade Intelectual, assinada em Estocolmo no dia 14 de julho de 1967;

"resultados da atividade intelectual"- objetos de propriedade intelectual e também resultados protegidos como informação confidencial; os resultados da atividade intelectual podem incluir soluções científicas, de *design*, técnicas e tecnológicas, software, banco de dados de computador, informação contida em documentação técnica e técnico-científica, bem como nos produtos desenvolvidos com fins militares, fabricados e fornecidos no curso da cooperação técnico-militar bilateral;

"propriedade intelectual precedente e outros resultados da atividade intelectual precedentes"- propriedade intelectual e outros resultados da atividade intelectual obtidos antes ou fora do marco da cooperação técnico-militar bilateral, pertencentes à República Federativa do Brasil ou a suas organizações autorizadas ou à Federação da Rússia ou a suas organizações autorizadas, cujo uso é necessário para implementar arranjos (contratos);

"propriedade intelectual e outros resultados da atividade intelectual em criação"- propriedade intelectual e outros resultados da atividade intelectual obtidos no curso da cooperação técnico-militar bilateral;

"informação"- dados referentes ao objeto do presente Acordo, bem como a arranjos (contratos) concluídos no curso da cooperação técnico-militar bilateral, incluídos seu cumprimento ou seus resultados obtidos, independente da forma de sua apresentação;

"informação confidencial"- informação (incluindo informação que constitui segredo comercial e *know-how*) que possui valor comercial efetivo ou potencial em razão de sua confidencialidade, desconhecida por terceiros, que não é legalmente de acesso livre e cujo detentor tenha tomado medidas para mantê-la confidencial;

"organizações autorizadas"- entidades legais da República Federativa do Brasil ou da Federação da Rússia que são autorizadas de acordo com suas legislações nacionais a levar a cabo comércio exterior relativo a produtos para fins militares.

Artigo 3

Os órgãos das Partes autorizados a implementar o presente Acordo serão:

pela Parte brasileira - Ministério da Defesa da República Federativa do Brasil;

pela Parte da Rússia - Ministério da Justiça da Federação da Rússia juntamente com o Ministério da Defesa da Federação da Rússia.

Em caso de transferência da autoridade a outro órgão durante a implementação do presente Acordo, ou mudança do nome do órgão autorizado, a respectiva Parte informará a outra Parte por via diplomática.

Os órgãos autorizados das Partes, mediante entendimento mútuo, estabelecerão, quando necessário, instância conjunta para discutir questões referentes à implementação deste Acordo.

Artigo 4

A cooperação das Partes na proteção da propriedade intelectual e de outros resultados da atividade intelectual no âmbito deste Acordo será implementada por meio de:

a) coordenação de questões relacionadas à proteção da propriedade intelectual e de outros resultados da atividade intelectual, observando a legislação nacional das Partes, conforme aplicável;

b) implementação de medidas para impedir e reprimir violações referentes à propriedade intelectual e a outros resultados da atividade intelectual, observando a legislação nacional das Partes, conforme aplicável;

c) implementação de medidas para impedir a divulgação e o uso não-autorizados de informação confidencial;

d) intercâmbio regular de experiência e informação sobre a proteção da propriedade intelectual e de outros resultados da atividade intelectual;

e) fornecimento de informação, a pedido da outra Parte, sobre atos normativos que regulamentem o uso e a proteção da propriedade intelectual e de outros resultados da atividade intelectual;

f) outras formas de cooperação acordadas pelas Partes.

Artigo 5

Nos arranjos (contratos) concluídos no curso da cooperação técnico-militar bilateral, as Partes ou as organizações autorizadas acordarão ou considerarão:

a) propriedade intelectual e outros resultados da atividade intelectual, cuja transferência ou uso seja previsto no curso da implementação;

b) alocação de direitos de propriedade intelectual e de outros resultados da atividade intelectual em desenvolvimento, levando em consideração a contribuição de cada Parte ou organização autorizada;

c) obrigações concernentes à aquisição ou à manutenção da proteção da propriedade intelectual e de outros resultados da atividade intelectual;

d) condições e abrangência do uso da propriedade intelectual e de outros resultados da atividade intelectual no território da República Federativa do Brasil, no território da Federação da Rússia e no território de terceiros estados;

e) direitos de cada Parte ou de organizações autorizadas de usar e transferir informação confidencial, e obrigações de garantir sua proteção;

f) procedimento para ressarcimento de danos causados pela revelação não-autorizada de informação confidencial, bem como pelo uso ilegal de propriedade intelectual e de outros resultados da atividade intelectual em desconformidade com arranjos (contratos);

g) condições e procedimentos de transferência, de intercâmbio e de publicação de informações sobre propriedade intelectual e sobre outros resultados da atividade intelectual.

Artigo 6

Em cumprimento às legislações pertinentes da República Federativa do Brasil e da Federação da Rússia, bem como aos tratados internacionais dos quais a República Federativa do Brasil e a Federação da Rússia são partes, cada Parte tomará medidas para impedir o uso não-autorizado da propriedade intelectual e de outros resultados da atividade intelectual, cujos direitos pertençam à República Federativa do Brasil ou às suas organizações autorizadas ou à Federação da Rússia ou às suas organizações autorizadas durante o desenvolvimento, a fabricação e a distribuição de produtos para fins militares nos territórios da República Federativa do Brasil e da Federação da Rússia e de terceiros estados.

Uma Parte ou suas organizações autorizadas não transferirão a uma terceira parte a propriedade intelectual e outros resultados da atividade intelectual recebidos da outra Parte ou de suas organizações autorizadas, nem a propriedade intelectual e outros resultados da atividade intelectual em desenvolvimento, sem a prévia autorização escrita da Federação da Rússia ou da República Federativa do Brasil, respectivamente.

Cada Parte ou suas organizações autorizadas não modernizarão produtos com fins militares para uma terceira parte sem o consentimento prévio escrito da República Federativa do Brasil ou da Federação da Rússia, respectivamente, caso, no curso da referida modernização, a propriedade intelectual e os outros resultados da atividade intelectual pertencentes à outra Parte e transferidos no marco da cooperação técnico-militar sejam usados.

Artigo 7

As Partes ou suas organizações autorizadas determinarão, por meio de mútuo acordo, a conveniência de patentear os resultados da atividade intelectual em desenvolvimento ou de reservá-los no formato de informação confidencial. Pedidos de patente serão submetidos conforme o procedimento seguinte:

a) pedidos de registro de resultados patenteáveis de atividade intelectual obtidos no curso da cooperação técnico-militar bilateral, desenvolvidos no território da República Federativa do Brasil, serão submetidos, primeiramente, às autoridades competentes a examinar tais pedidos, de acordo com a legislação da República Federativa do Brasil;

b) pedidos de registro de resultados patenteáveis de atividade intelectual obtidos no curso da cooperação técnico-militar bilateral, desenvolvidos na Federação da Rússia, serão submetidos, primeiramente, aos órgãos executivos federais competentes a examinar tais pedidos, em consonância com a legislação da Federação da Rússia.

Artigo 8

Se uma das Partes ou suas organizações autorizadas considerar que a propriedade intelectual e outros resultados da atividade intelectual em desenvolvimento não sejam passíveis de proteção pela legislação da República Federativa do Brasil ou da Federação da Rússia, os órgãos autorizados ou as organizações autorizadas da República Federativa do Brasil e da Federação da Rússia estabelecerão, imediatamente, consultas sobre sua proteção e uso, por meio de arranjos (contratos).

A propriedade intelectual precedente e outros resultados da propriedade intelectual de uma das Partes ou de suas organizações autorizadas que não

possa ser protegida sob a legislação nacional em propriedade intelectual da outra Parte estará sujeita a outra legislação aplicável desta outra Parte.

A transmissão de propriedade intelectual precedente e de outros resultados da atividade intelectual somente poderá ser feita após terem sido tomadas medidas para garantir sua proteção legal.

Uma Parte ou suas organizações autorizadas serão solicitadas pela outra Parte ou suas organizações autorizadas a apresentar informação, que possa ser transmitida, sobre titularidade de direitos de propriedade intelectual precedente, cuja transferência ou uso seja prevista quando da conclusão de arranjos (contratos).

Artigo 9

Informação sobre questões relativas à cooperação técnico-militar bilateral, reconhecida como confidencial pela Parte ou por sua organização autorizada que transmite a informação, será automaticamente considerada confidencial e protegida como tal pela outra Parte ou por sua organização autorizada que recebem essa informação, desde que a Parte receptora ou sua organização autorizada seja previamente informada a respeito da confidencialidade da informação.

As modalidades de intercâmbio e proteção mútuos de informação classificada serão determinadas por acordo em separado entre o Governo da República Federativa do Brasil e o Governo da Federação da Rússia.

Artigo 10

O presente Acordo não modifica a regulamentação legal da propriedade intelectual das Partes, determinada pela legislação pela legislação da República

Federativa do Brasil ou da Federação da Rússia, respectivamente. Ademais, o Acordo não prejudicará as obrigações internacionais das Partes.

Artigo 11

Quaisquer controvérsias ou diferenças entre as Partes em relação à implementação e interpretação do presente Acordo será resolvida por meio de consultas e negociações entre as Partes.

Artigo 12

O presente Acordo pode ser emendado e complementado na forma de protocolos separados.

Artigo 13

O presente Acordo terá duração indeterminada e entrará em vigor 30 dias após o recebimento da última notificação escrita, por via diplomática, sobre o cumprimento, pelas Partes, de seus respectivos procedimentos internos para a entrada em vigor do presente Acordo.

Qualquer Parte poderá denunciar o presente Acordo enviando, por via diplomática, notificação escrita à outra Parte. O presente Acordo cessará seus efeitos seis meses após a data de recebimento daquela notificação pela outra Parte.

A denúncia do presente Acordo não afetará o cumprimento das obrigações estabelecidas para as Partes pelos Artigos 6 e 9 do presente Acordo, exceto se as Partes decidirem o contrário.

Feito em Moscou, no dia 14 de maio de 2010, em duas cópias originais, nos idiomas português, russo e inglês, sendo os três textos igualmente autênticos.

Em caso de divergência na interpretação do presente Acordo, o texto em inglês prevalecerá.

*****

ACORDO ENTRE O GOVERNO DA REPÚBLICA FEDERATIVA DO BRASIL E O GOVERNO DA FEDERAÇÃO DA RÚSSIA PARA COOPERAÇÃO NO CAMPO DA SEGURANÇA INTERNACIONAL DA INFORMAÇÃO E DA COMUNICAÇÃO

O Governo da República Federativa do Brasil
e
O Governo da Federação da Rússia,
doravante denominados Partes,

Considerando o desenvolvimento das relações entre a República Federativa do Brasil e a Federação da Rússia com base na confiança mútua e na cooperação;

Notando que progresso considerável tem sido alcançado no desenvolvimento e na aplicação das mais recentes tecnologias da informação e meios de comunicação;

Expressando preocupação com as ameaças advindas do possível uso de tais tecnologias e meios para propósitos inconsistentes com os objetivos de manutenção da paz, da segurança e da estabilidade internacionais nas esferas civil e militar;

Atribuindo grande importância à segurança internacional da informação e da

comunicação como um dos elementos-chave do sistema de segurança internacional;

Considerando o importante papel da segurança da informação e da comunicação para assegurar os direitos humanos e as liberdades fundamentais;

Considerando as resoluções da Assembleia Geral das Nações Unidas intituladas "Desenvolvimentos no campo da informação e das telecomunicações no contexto da segurança internacional";

Esforçando-se para enfrentar as ameaças à segurança internacional da informação e da comunicação, para assegurar os interesses das Partes relativos à segurança da informação e da comunicação e para criar um ambiente internacional de informação de paz, cooperação e harmonia;

Desejando estabelecer um arcabouço legal e institucional para cooperação entre as Partes no campo da segurança internacional da informação e da comunicação, e enfatizando a importância de tal cooperação para a continuidade do desenvolvimento de parceria bilateral estratégica,

Acordam o que se segue:

Artigo 1
Terminologia

1. Para o propósito da interação entre as Partes na implementação deste Acordo, os termos básicos a serem utilizados estão listados no Anexo, que constitui parte integral do presente Acordo.

2. O Anexo pode, se necessário, ser ampliado, emendado e atualizado conforme entendimento entre as Partes, por via diplomática.

Artigo 2
Ameaças Principais no Campo da Segurança Internacional da Informação e da Comunicação

As Partes cooperarão no âmbito deste Acordo, levando em consideração as seguintes ameaças principais à segurança internacional da informação e da comunicação:

1) uso dos meios e tecnologias da informação e da comunicação em conflitos internacionais com propósitos hostis nos campos militar e civil, incluindo danos a infraestruturas críticas;

2) uso dos meios e tecnologias da informação e da comunicação com propósitos e em atividades terroristas;

3) uso dos meio e tecnologias da informação e da comunicação com propósitos e em atividades criminosas;

4) uso de posição dominante no campo dos meios e tecnologias da informação e das comunicações em detrimento dos interesses e da segurança de outros Estados;

5) desastres naturais ou falhas tecnológicas que afetem a operação segura e estável das infraestruturas globais e nacionais de informação e de comunicação.

Artigo 3

Áreas Principais de Cooperação

As Partes cooperarão com base no presente Acordo nas seguintes áreas principais:

1) identificar, coordenar e implementar medidas conjuntas necessárias para assegurar a segurança internacional da informação e da comunicação;

2) estabelecer um arcabouço de cooperação para evitar, detectar, tratar e responder às ameaças mencionadas no Artigo 2 do presente Acordo;

3) realizar estudo, pesquisa e avaliação no campo da segurança da informação e da comunicação, incluindo a cooperação técnica e científica entre as Partes;

4) promover coordenação em diferentes foros de governança da Internet, em temas relacionados à segurança da informação e da comunicação;

5) assegurar a segurança da informação e da comunicação de infraestruturas críticas nacionais;

6) elaborar e implementar políticas coordenadas para o uso de assinatura digital e proteção da informação nas trocas internacionais de informação;

7) compartilhar informação a respeito da legislação da República Federativa do Brasil e da legislação da Federação da Rússia relativa à segurança da informação e da comunicação;

8) desenvolver e aperfeiçoar a base legal internacional e mecanismos práticos para cooperação entre as Partes no fortalecimento da segurança internacional da informação e da comunicação;

9) interagir no âmbito das organizações e dos foros internacionais em temas relativos à segurança internacional da informação e da comunicação;

10) compartilhar experiência, treinar especialistas, realizar reuniões de trabalho, conferências, seminários e outras foros de representantes autorizados e especialistas das Partes no campo da segurança da informação e da comunicação.

As Partes podem determinar outras áreas de cooperação por consentimento mútuo.

Artigo 4
Princípios Gerais de Cooperação

1. As Partes cooperarão no âmbito do presente Acordo para contribuir para o desenvolvimento econômico e social e para manter a paz e a segurança internacionais, de acordo com princípios geralmente reconhecidos e normas do direito internacional, incluindo os princípios da solução pacífica de controvérsias, do não-uso da força, da não-interferência em assuntos internos, do respeito aos direitos humanos e às liberdades fundamentais.

2. Cada Parte terá direitos iguais de proteger os recursos de informação e as infraestruturas críticas de seus Estados das ameaças mencionadas no Artigo 2

do presente Acordo.

Artigo 5
Implementação

1. Após sessenta dias da entrada em vigor do presente Acordo, as Partes trocarão informações relativas às autoridades competentes da República Federativa do Brasil e da Federação da Rússia responsáveis pela implementação do presente Acordo e aos canais de intercâmbio direto de informação sobre áreas específicas de cooperação.

2. Com vistas a examinar a implementação do presente Acordo, a possibilitar o intercâmbio de informação, a análise e a avaliação conjunta das novas ameaças à segurança da informação e da comunicação, bem como determinar, acordar e coordenar medidas de resposta conjuntas, as Partes deverão manter consultas regulares entre os representantes autorizados e as autoridades competentes da República Federativa do Brasil e da Federação da Rússia (doravante - consultas).

3. Consultas regulares serão realizadas duas vezes ao ano na República Federativa do Brasil e na Federação da Rússia em caráter rotativo.

4. Qualquer Parte poderá propor consultas adicionais e sugerir data, lugar e agenda.

5. As Partes poderão estabelecer interação prática em áreas específicas de cooperação possibilitada pelo presente Acordo, por meio das autoridades competentes da República Federativa do Brasil e da Federação da Rússia,

responsáveis por implementar este Acordo.

6. Com vistas a regulamentar a cooperação em modalidades específicas, as autoridades competentes da República Federativa do Brasil e da Federação da Rússia poderão concluir os ajustes complementares apropriados.

Artigo 6
Proteção da Informação

1. O presente Acordo não obriga as Partes a fornecer informações no contexto da cooperação nos termos do presente Acordo e não respalda a transferência de tais informações caso sua divulgação possa ser nociva aos interesses nacionais.
2. Os procedimentos para proteção das informações classificadas que possam ser consideradas necessárias em certos casos para a implementação do presente Acordo deverão ser reguladas em conformidade com os acordos relevantes firmados entre as Partes.

3. As informações transferidas ou geradas no curso da cooperação no âmbito do presente Acordo não serão divulgadas ou transferidas sem o consentimento por escrito da Parte que originou as informações.

Artigo 7
Recurso Financeiros e Outros Recursos

1. As Partes assumirão, independentemente, os custos da participação de seus respectivos representantes e especialistas nas atividades relativas à implementação do presente Acordo.

2. As Partes poderão acordar outros procedimentos de custeio, em cada caso particular, conforme a legislação da República Federativa do Brasil e a legislação da Federação da Rússia.

3. Todas as atividades realizadas no contexto do presente Acordo estarão sujeitas à disponibilidade de recursos financeiros, humanos e outros recursos apropriados de cada Parte.

Artigo 8
Relação com Outros Tratados Internacionais e com a Legislação Nacional

1. O presente Acordo não afetará direitos e obrigações das Partes advindos de outros tratados internacionais dos quais seus respectivos Estados sejam parte.

2. Todas as atividades realizadas no âmbito do presente Acordo estarão sujeitas às leis e regulamentos nacionais em vigor para cada Parte.

Artigo 9
Solução de Controvérsias

Controvérsias que possam surgir entre as Partes sobre a interpretação ou a aplicação do presente Acordo serão solucionadas por meio de negociações e consultas entre as autoridades competentes e, se necessário, por via diplomática.

Artigo 10
Idiomas de Trabalho

Os idiomas de trabalho para cooperação no âmbito do presente Acordo serão o português, o russo e o inglês.

Artigo 11

Entrada em Vigor, Duração, Término e Emendas

1. O presente Acordo entrará em vigor no trigésimo dia após a data de recebimento, por via diplomática, da última notificação por escrito de que foram cumpridos pelas Partes os respectivos procedimentos internos necessários para sua entrada em vigor.

2. O presente Acordo permanecerá em vigor por período indeterminado.

3. O presente Acordo poderá ser emendado, a qualquer tempo, por consentimento escrito de ambas as Partes, que será formalizado por via diplomática. A entrada em vigor das emendas ao presente Acordo estará sujeita ao mesmo procedimento para a entrada em vigor deste Acordo.

4. O presente Acordo poderá ser denunciado noventa dias após o recebimento, a qualquer tempo, por uma Parte, por via diplomática, de notificação por escrito da outra Parte de sua intenção de denunciar o Acordo.

5. Em caso de denúncia do presente Acordo, as Partes continuarão vinculadas às disposições do Artigo 6, com respeito a quaisquer informações obtidas no âmbito do presente Acordo. A denúncia não afetará a implementação das atividades de cooperação realizadas no âmbito do presente Acordo e não completadas no momento de sua denúncia, a não ser que as Partes acordem de outra forma.

Feito em Moscou, em 14 de maio de 2010, em duplicata, nos idiomas português, russo e inglês, sendo todos os textos igualmente autênticos. Em caso de divergência na interpretação das disposições do presente Acordo, o texto em inglês prevalecerá.

ANEXO ao Acordo entre o Governo da República Federativa do Brasil e o Governo da Federação da Rússia para Cooperação no Campo da Segurança Internacional da Informação e da Comunicação

LISTA DE TERMOS BÁSICOS NO CAMPO DA SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO "SEGURANÇA DA INFORMAÇÃO E DA COMUNICAÇÃO" – PROTEÇÃO DO INDIVÍDUO, DA SOCIEDADE, DO ESTADO E DE SEUS INTERESSES CONTRA AMEAÇAS POTENCIAIS E EXISTENTES NO CAMPO DOS MEIOS E TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO, INCLUINDO MEDIDAS PARA ASSEGURAR DISPONIBILIDADE, INTEGRIDADE, CONFIDENCIALIDADE E AUTENTICIDADE DA INFORMAÇÃO

1. Segurança da informação e da comunicação – proteção do indivíduo, da sociedade, do Estado e de seus interesses contra ameaças potenciais e existentes no campo dos meios e tecnologias da informação e da comunicação, incluindo medidas para assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação.

2. Ameaça à segurança da informação e da comunicação – fatores que representam ameaça ao indivíduo, à sociedade, ao Estado e aos seus interesses

relativa aos meios e tecnologias da informação e da comunicação.

3. Infraestrutura da informação e da comunicação – conjunto de meios técnicos, sistemas, instalações e pessoal envolvidos na geração, desenvolvimento, transformação, transmissão, uso e armazenamento de informação.

4. Recursos de informação – infraestrutura da informação, bem como a informação em si e seus fluxos.

5. Infraestruturas críticas – instalações físicas, sistemas, serviços e instituições cujo dano ou destruição causará sério impacto à ordem social, econômica e política ou à segurança nacional.

6. Segurança internacional da informação e da comunicação – ambiente de relações internacionais que rechaça a violação da estabilidade mundial e as ameaças à segurança dos Estados e da comunidade mundial no campo dos meios e tecnologias da informação e da comunicação.

3.3. Análise dos resultados parciais

O resultado inicial de minha Iniciação Científica foi embasado no conceito de cyberwar. Para analisar sua procedência, usei o livro *Wired for war: the robotics revolution and conflict in the 21st cintura* de P. W. Singer e para entender o conflito como acontece hoje, me ative ao livro *Cyber war: the next threat to national security and what to do about it* de Richard Clarke e Robert K. Knake. Richard Clarke coloca a cyber guerra como a invasão de redes de uma nação, por ou em nome de outra nação, ou qualquer outro tipo de atividade que afete um sistema operacional, no caso de alteração ou falsificação de informação ou danificação do mesmo sistema.[1]

Em seguida, com a leitura de *Estados de Violência - Ensaio Sobre o Fim da Guerra* de Frédéric Gros, foi possível entender a cyber guerra como elemento dos estados de violência, visto que este tipo de conflito não se encaixa no conceito clássico de guerra.

Para Gros, os conflitos pós-modernos já não são mais redutivos à antiga definição de guerra, que seria lutada por exércitos convencionais e batalhas bem definidas. Os novos conflitos vêm acompanhados de novos atores: mercenários, exércitos privados, "senhores da guerra", as grandes potências em suas intervenções, terroristas, e neste caso, os *cyberwarriors*.

O novo regime dos estados de violência é resultado, segundo Gros, das novas pressões e poderes do mundo contemporâneo, como a imagem de vítimas, o fluxo de riquezas e pessoas, a multiplicação de violências; Gros aponta a mídia e a mundialização como possíveis responsáveis de muitos dos

[1] CLARKE, Richard e KNAKE, Robert K. *Cyber war*: the next threat to national security and what to do about it. Nova Iorque: HarperCollins, 2010. Capítulo 1.

novos embates e questiona não só as mudanças políticas e econômicas fomentadas pela globalização, mas também a mudança que esta causa nos estados de violência.

Por fim, o autor coloca o fim da guerra dentro dos estados de violência como o possível tempo de segurança, ou seja, os novos métodos de segurança se tornam o ator regulatório do novo regime dos estados de violência.

O paralelo entre o ensaio de Frédéric Gros e as leituras realizadas mostra como a cyber guerra faz parte do novo regime dos estados de violência, por mais que tenha provenha das inovações no combate das chamadas guerras clássicas, foi com a mundialização que a nova forma de conflito se estabeleceu e dela surgiram novos atores dos conflitos pós-modernos. Surge a questão do anonimato, das guerras "lutadas" as distancia com as novas tecnologias de guerra, questões que afastam a cyber guerra da definição de guerra clássica.

A análise das estruturas burocráticas dos Estados Unidos e do Brasil se torna relevante nesse momento, vista a crescente importância das agendas de segurança, que nesse novo períodos são o que garantem a ausência de guerra, e também esbarram na obra de Clarke, que tenta estruturar uma agenda palpável e própria para conflitos cibernéticos.

A Organização de Cooperação de Xangai, pioneira na discussão e formulação de estratégias de combate aos crimes cibernéticos, marca o início do desenvolvimento de medidas de *cybersegurança*. O Acordo de Não-Agressão por Armas de Informação, firmado por Brasil e Rússia, demostra também o papel do Brasil nessa nova discussão e a importância de uma agenda de segurança sobre o tema dentro do país, visto os diversos ataques ocorridos especialmente durante o ano de 2011 por hackers a sites governamentais.

Segundo Gros, os estados de violência e dos novos tipos de conflitos são regulados por ações voltadas à segurança, processos de prevenção, e as agendas de segurança, dessa forma os novos tratados, acordos e alianças referentes à cybersegurança são de extrema importância na discussão. Eles tem a função de minimizar riscos, já que os novos conflitos não necessáriamente envolvem o combate direto, como antes.

Esse novo quadro de conflitos pós-modernos nos obrigam a pensar novos vigilantes, e novas formas de defesa. Os *serious games* são um exemplo dessa nova iniciatica, já que buscam *cyberwarriors* dentro de suas casas e colocam a população próxima aos multiplos conflitos existentes no mundo. Ao mesmo tempo, a busca e contratação de hackers pelos governos, dentro de suas agências de segurança, mostram como as resistências estão sendo assimiladas nos novos estados de violência.

Minha pesquisa procurou mostrar a procedência da cyberwar, e assim da cybersegurança, a partir do modelo clássico de guerra. Em seguida, apresentar as reações para a nova forma de conflito: a mudança e adaptação das estruturas burocráticas de países como os Estados Unidos e o Brasil, o início da discussão da cybersegurança na Organização de Cooperação de Xangai, e o acordo firmado pelo Brasil, mostrando como o tema é discutido em nosso país. Em seguida, os serious games mostram como a guerra e os conflitos são lutados de forma distinta, e como o recrutamento e relação da população com os mesmo também se alterou.

Procurei embasar a discussão na análise teórica de Fredéric Gros sobre os novos Estados de Violência e os conflitos pós-modernos. Como explicitado anteriormente, Gros mostra o abandono do conceito clássico de guerra e aponta seus novos agentes, componentes e resistências necessárias para que os novos

conflitos sejam solucionados.

3.3. Bibliografia

CANOGIA, Claudia e MANDARINO, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação.

CLARKE, Richard e KNAKE, Robert K. *Cyber war*: the next threat to national security and what to do about it. Nova Iorque: HarperCollins, 2010.

HALPIN, Edward (et al). *Cyberwar, netwar and the revolution in military affairs*. Nova Iorque: Palgrave McMillan, 2006.

SINGER, P. W. *Wired for war*: the robotics revolution and conflict in the 21st century. Nova Iorque: The Pinguin Press, 2009.

GROS, Frédéric. *Estados de Violência - Ensaio Sobre o Fim da Guerra.* Editora Idéias & Letras.

LUCERO, Everton. Governança da Internet: Aspectos da Formação de um Regime Global e Oportunidades para a Ação Diplomática. Brasília: Fundação Alexandre de Gusmão, 2011.

The Shanghai Cooperation Organization. SIPRI Policy Paper no. 17. Alyson J. K. Bailes, Pál Dunay, Pan Guang e Mikhail Troitskiy.

3.4. Netnografia

http://www.goarmy.com

http://www.americanarmy.com

http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=22683&sid=18

http://www1.folha.uol.com.br/folha/brasil/ult96u392530.shtml

http://www.dhs.gov/

http://news.bbc.co.uk/2/hi/technology/2889171.stm

http://www.sectsco.org/EN/

http://www2.cultura.gov.br/programas_e_acoes/cultura_e_pensamento/noticias/agenda/index.php?p=28594&more=1&c=1&pb=1

http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/atos-assinados-por-ocasiao-da-visita-do-presidente-luiz-inacio-lula-da-silva-a-russia-2013-14-de-maio-de-2010/?searchterm=tratado%20russia%20brasil

http://www.globalsecurity.org/military/world/int/sco.htm

http://www.cgi.br/regulamentacao/resolucao2009-003.htm

http://www.senado.gov.br/noticias/os-dez-principios-para-a-internet.aspx

http://www.senado.gov.br/noticias/Jornal/noticia.asp?codEditoria=2467&dataEdicaoVer=20110609&dataEdicaoAtual=20110609&nomeEditoria=Justi%C3%A7a

http://www.cgi.br/

http://www.youtube.com/watch?v=s1V7jBACLQE

www.globalconflicts.eu/

www.conflitosglobais.com.br/