Position of the State of Israel for the purpose of the conference held by Forum for 21st Century on 29 November 2011 reflected in the second draft of the negotiation paper, regarding the Global Cyber Security issues.

After in-depth analysis of the second draft proposed by *The Forum for 21st Century* let the State of Israel submit its position including suggestions about selected topics.

- With all the respect to *the Forum* for 21st Century and especially to all participating parties, the State of Israel feels the necessity of reminding the core issue of this conference with the help of the words of a great man, Benjamin Franklin who said, ,,*by failing to prepare, you are preparing to fail.*"

- It does not mean that the participating parties are preparing to fail. On the contrary, the vision of this quote is to prevent of such a failure. *The Forum* has to stay careful, pragmatic, allowing further discussions in accordance with short and long-term visions, however the crucial point of present discussion is to determine our very next steps, with ***practical*** respect to the relatively newly formed issue and to the variousness of participating parties, their relations and interests.

- Past decades, we have been witnesses on how cyberspace affects our everyday lives. The internet has transformed how we do business, opening up markets, connects economies as never before. Digital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies. Information technology is fostering transnational dialogue and facilitating the global flow of goods and services. Critical life-sustaining infrastructures that deliver electricity and water, control air traffic, and support our financial system all depend on networked information systems. Moreover, it had changed social relations, how we communicate with one another, with a friend down the street or a colleague across the globe.

- On the other hand, simultaneously with the development of the cyberspace for the peaceful purposes, improvement for the daily use, there is a new space for wide range threats. Such cyber-attacks include acts of cyber war, terrorism, espionage, protest, vandalism and more. Lines between categories are often blurred, it is not easy to identify the perpetrators, but not impossible, as well as understand their motives. Nowadays, as more than two thirds of all humanity uses digital communications, anybody with a computer has the potential to inflict harm. It is crucial to realize all possible threats, and their reasons, such as costs, possibility to hide the personality, location, affecting large number of people and targets. There are no barriers or check points, and such attack could be done from anywhere in the world.

- The State of Israel welcomes the effort of *The Forum* of creating proposals and ideas involved in the second draft. Nevertheless, as it is mentioned above, at this stage of solving the issue that touches us all, it is crucial to be and look at it from the practical perspective.

- There is a strong need of analyzing the ways of fighting such malevolent behavior. And according to that adjust further cooperation amongst parties.

  - As the primary way of blocking attempts and dealing with actions, we want to point out at the *technological means*. The very first and most common protection in this field, amongst governments, private sector is well-known *firewall*. It is crucial to develop this system on a daily base, as well as other used methods like various *spy-bots*, *traps*, *data-collective Trojans*, etc.

  - Secondary matter connects to the *individual terrorists*, or even *hacktivist groups*, in which we see prospective cooperation as long as the fact taken into consideration, that every malevolent individual, especially famous hackers have their own techniques of hacking, notable amongst the best of them.

  - The tertiary method of fighting cybercrime reflects the need of financial aid for such activities. Countries should cooperate in analyzing the private donors and organizations responsible for these actions and intervene effectively.

  - The last, but the hardest one, in means of achievement, we consider is, so-called *Internal discipline*. The point of this propose is to prevent of using unknown digital devices and flash memories, in the companies, governance offices, and everywhere, where such attack could be expected. Regarding to the complexity of achievement risk-free behavior, we suggest the application of this *discipline rule* to be the discretion of corporations, governments and individuals.

- The State of Israel understands the necessity, and is willing to discuss the legal basis and terms with respect to usage of the Internet and local intranets, although we propose to remove the term *control* from the further discussions, since we believe that this point should be discussed on the national level. Moreover, with respect to all parties, we want to point out at the fact, that the legal basis and terms has already been the matter of the national and international dialogues, and therefore we propose the revision of the existing documents and terms, that has been already adopted by specific conventions engaged in this issue.

- To the point of creation International Cyberlaw, the State of Israel stands the position, where it is important to realize its long-term creation, costs, formulations, associated to the interpretation of the law by each country, and especially, whether such ***Cyberlaw*** is able to exist at all under present conditions.

- Therefore, as mentioned in the beginning of this position, we suggest to all parties to take into consideration the reality, in which we have to act today. Regarding to this, we propose further discussions of creating specific *Cyber Issues Convention*, in which signatories´ further cooperation will be taken into account, as well as proposed *Basic Cyberspace Principles*. We believe that the status of Human Rights must be set in this convention. In this phase, it is important to set up our actions against malevolent actions, from the financial point of view, and mainly to strengthen the positions and methods on this battlefield. The nations need to develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks.

    - We agree with the statements of users´ internet privacy, as well as we see with favour the prevention of deprivation of having access to the Cyberspace, unless the national security is endangered. The case of endangering national security and further consequences we suggest to consult on the national level.

- In respect to the monitorship of companies which profit from personal data collecting, the State of Israel propose supervising these companies by state representatives and representatives of NGO's (multi-stakeholder model) rather, than strictly regulating and controlling them.

- As we begun this statement with the respect of looking at the issue from the practical and pragmatic side, and the fact that we live in market economy and democracy, we would like to hear from *The Forum* further specification of proposed „hard sanctions" as well as „economic reasons", because the use of *self-motivated reasons* to submit personal data into the cyberspace, and follow-up marketing calculations, through the *social sites*, and internet *clicks*, is the corner stone of e.g. *Facebook Ads* or *Google Ads* that are used worldwide.

- The State of Israel and Jewish people still suffers from what happened in the past. The Holocaust was the worst crime of all times, and will be remembered forever! It happened because of ignorance of the facts that leads to this tragedy. Nowadays, there could be found people that continually deny what happened, going even further proclaiming of *vanishing* the Holy Land. Despite the respect of expression, do *The Forum* thinks that statements like these are morally fine?

    - We would like to pass for the further discussion the point that speaks about *freedom of opinion* and *expression*, determined by law. An issue that is being respected amongst all democratic countries, whether it is a political opposition, movement or simply, any human being. According to this, we feel responsible to raise the question about non-democratic regimes, since they follow their own laws.

- As mentioned above, instead of creating new definition of Cyberspace and terms related to this, we propose the revision and updating of the existing ones, including human rights, principles, sanctions and further discussed conclusions that will be included in proposed *Convention*.

- We agree with the differentiation of sanctions in accordance with the type of criminal or illegal activity conducted. We believe that this issue must be discussed with all participating parties, and that is why we demand this point be included in the further rounds of *The Forum.*

- The idea of a *Joint Cybercriminal Database* is an important idea, however we find it to be one of the long-termed goals of cooperation between countries. From the point of view of the very close future we believe and suggest focusing rather on bilateral cooperation in terms of joint database. Today, before cooperating we must answer the question of trust. For instance, do United States trust enough Russia to change sensitive information? What about the confidence between China and India? And other countries. Moreover, we have to take into consideration the fact that databases which include wide range information are much more vulnerable to the outer world, also because of the exclusivity of the successful attack. In addition, we see the importance of finding ways of closer cooperation, and technological capabilities in order to sufficiently secure the future *database.*

- Nevertheless, that attacks could stay on a cheaper level, costs of fight against them are raising rapidly. We would like to point out the financial issue according to the creation of any new body in international society. Furthermore there are other requirements of establishment proposed *CYBERPOL*, e.g. time, people involved, legislative framework, structure, that needs consensus, which would be complicated to achieve, at least in a reasonable period of time. With the respect of the shortance of time, and all others conditions, we propose of strenghten the powers of the *INTERPOL IT Crime Steering Committee.* The structure of this Commitee consists of representatives of the government, major IT security companies and academia. We believe that the aims of the *Commitee* will be the matter of further negotiations with the respect to already given ones, e. g. harmonizing and providing guidance to regional working party activities, facilitate partnerships between the different sectors involved in the fight against cybercrime. We see with favour the fact, that the *INTERPOL´s* cybercrime activities should revolve around three main pillars: operations, training and research and development.

    - The idea of *Best Practice Sharing* can be useful, but again, we suggest to stay on bilateral level in the present, with coordinating actions and building trust amongst countries for implement this idea in the future. On the other hand, we stand the position that IT companies will not be willing of sharing, basicaly their know-how and techniques.

- At this phase of the statement, the State od Israel would like to point out, with the respect of *users´ computer skills*, at the phrase „strange activity“, where we are not confident of correct detection of such activities, hence we apply on *The Forum* for closer definition.
    - We consider the proposal of *Internet ID Numbers* to be qualified for next discussion between the parties involved in *The Forum*.

- The State of Israel, as the only one democratic country in the region, declares the reservation of the right to act against malevolent and destructive attacks on its national defense systems, economic bodies, vital infrastructure and government bodies, since experiencing regular attempts.

- As mentioned above in the text, we support cooperation in prosecution of illegal paramilitary groups, terrorist organizations and individuals behind hacktivism, however we see irrelevant the distinction *between military units* and *organized individuals* as proposed by *The Forum*, since it is possible to meet the expanded cooperation of such individuals with governments world wide. Moreover, it is crucial to realize, that fighting against cyberterrorism and cybercrime must be interconnected with the private sector or individual cyber-experts.