A. Key Principles to Guide Capacity-Building Initiatives & Current Concerns for Developing Countries

The importance of capacity-building efforts has been established as a key pillar of the normative framework for responsible state behaviour in cyberspace in the Open-Ended Working Group's (OEWG) Annual Progress Report (2021).[1] The OEWG's substantive sessions have also seen several member-states unanimously and consistently advocate for the development of international and regional-level capacity-building efforts. However, different member-states have put forth a wide range of priority action items such as securing critical infrastructure of countries, establishing CERT's, cyber crisis management mechanisms and building secure physical infrastructure for Information and Communication Technologies (ICT). Commonly agreed upon principles to guide the development of such initiatives include sustainability, purpose and results-oriented agendas, evidence-based frameworks, transparency, non-discriminatory, politically neutral cooperation, sovereignty respecting, universality, and equity in the facilitation of access to ICTs.[2]

It is important for cyber capacity-building activities at the international level to correspond with national needs and priorities that can be benchmarked against globally determined baselines. For example, many member-states have advocated the use of UK's Oxford's Cybersecurity Capacity Maturity Model[3] as a framework for countries to assess their cybersecurity ecosystems and identify gaps and appropriate strategies. The use of these frameworks is particularly useful in the context of cyber capacity-building for developing countries. Insights from such assessments at national levels can be used to identify a common development agenda for regional and international level efforts to help developing countries receive the assistance they need, and develop ICT capacity to improve and secure their cyber growth. It has been established that targeted capacity-building that improves respective national competencies is necessary for the implementation of the OEWG's normative framework. Public-private partnerships have also been

[1] A/AC.290/2021/CRP.2, Final Substantive Report, Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, United Nations General Assembly <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>
[2] Centre for Communication Governance, 'Reflections on Second Substantive Session of UN OEWG on ICT Security (Part 3): Confidence Building Measures, Capacity Building and Institutional Dialogue' (*The CCG Blog*, 22 June 2022) <https://ccgnludelhi.wordpress.com/2022/06/22/reflections-on-second-substantive-session-of-un-oewg-on-ict-security-part-3confidence-building-measures-capacity-building-and-institutional-dialogue/>
[3] 'The Cyber Maturity Model' (*Global Cyber Security Capacity Centre*) <https://gcscc.ox.ac.uk/the-cmm>

highlighted as a key priority area, particularly for the skilling of cyber professionals, exchange of threat intelligence and exchange of technical knowledge.[4]

Multistakeholder approaches to capacity-building initiatives at regional and international levels can help build a global culture for cybersecurity that is sustainable, and inclusive while strengthening institutional cooperation and dialogue. For instance, civil society organisations are essential in offering feedback on the state of cyber threats, particularly regarding matters like how cyberattacks affect safety, human rights, and vulnerable demographics. Multistakeholder initiatives that involve cybersecurity incident exercises, assisting in the establishment of national or regional points of contact networks, exchanging information in targeted discussions, and enhancing the ability of States and stakeholders to support widespread accountability in cyberspace are examples of good practices in this regard.

There has been discourse around the need for distinctions to be made between capacity-building efforts that aim to bridge the digital divide, and those that are aimed towards implementation of normative cyber capacity frameworks. This difference arises from the need to equip developing countries with a baseline level of cyber capacity tools and technologies before they are able to implement and partake in other capacity-building initiatives and efforts. There is thus a need to prioritise practical support by establishing capacity-building programs in developing countries to mitigate ICT risks and build their preparedness to respond to cyberthreats effectively. This includes equipping developing countries with the required knowledge, training and best practices regarding establishment of national level cybersecurity strategies, CERT's, cyber diplomacy engagement mechanisms etc.

Towards this end, it can be helpful to harmonise capacity-building programmes for developing countries with bilateral and regional efforts. For example, the conduct of fellowships, workshops, training programmes, education courses, etc., by countries with advanced ICT capabilities can be used as platforms for technical capacity-building for State officials/experts in developing countries. There have been recommendations by member-States at the OEWG for the United Nations Institute of Disarmament Research (UNIDIR) to assume the role of mapping global and regional cyber capacity-building efforts, spanning financial support and technical assistance,

[4] 'Public-Private-Civil Partnerships in Cyber Capacity Building' (Digital Watch Observatory, 2 December 2021) <<https://dig.watch/event/13th-internet-governance-forum/public-private-civil-partnerships-cyber-capacity-building>>

aimed at compiling a list of best practices. Disaster and climate resilience of ICT infrastructure in developing countries is another key area of concern.

B. India's Positioning on Capacity-Building at the UN OEWG

India has made various recommendations to the OEWG on the security of and in the use of ICTs under the theme of capacity-building initiatives. Some of these include:[5]

- The need for capacity-building measures to be targeted at technical and policy agencies at the national level.
- Funnelling capacity-building through regular institutional dialogue to ensure inclusivity, neutrality and trust.
- Establishing a forum of CERTs, under the UN, to facilitate tabletop exercises, critical infrastructure security, general cybersecurity awareness campaigns, and cyber threat preparedness.
- Establishing an international counter task force comprising international experts in order to provide technical assistance and infrastructural support for cyber defense and cyber incident response against critical infrastructure threats.

In the context of capacity-building efforts, India has advocated the need for a permanent mechanism to be established under the United Nations to prepare an action-oriented programme for small and developing countries to develop their ICT capabilities.[6] The need for tailored capacity-building efforts to bridge the digital divide has been highlighted as a key priority by the Indian delegation at the OEWG.[7]

Towards this, India made a proposal for a Global Cyber Security Cooperation Portal (GCSCP)[8] that would contain a document repository, a PoC directory, a mapping of the needs of states in

---

[5] Centre for Communication Governance, 'Reflections on Second Substantive Session of UN OEWG on ICT Security (Part 3):Confidence Building Measures, Capacity Building and Institutional Dialogue' (*The CCG Blog*, 22 June 2022) <https://ccgnludelhi.wordpress.com/2022/06/22/reflections-on-second-substantive-session-of-un-oewg-on-ict-security-part-3confidence-building-measures-capacity-building-and-institutional-dialogue/>
[6] Ministry of External Affairs India, Statement at the OEWG, July 2022 <https://documents.unoda.org/wp-content/uploads/2022/07/India-Statement-28-July-22.pdf>
[7] India's Statement on "The Centrality of International Cooperation and Capacity Building in Building Safe and Secure Cyberspace", August 2022 (Ministry of External Affairs) <https://eoi.gov.in/eoisearch/MyPrint.php?15202%3F001%2F0002>
[8] Working Paper on Global Cyber Security Co-operation Portal, Permanent Mission of India to OEWG <https://docs-library.unoda.org/Open-

capacity-building, a calendar of conferences and workshops, and incident reporting.[9] The GCSCP is expected to provide an 'integrated' platform for the sharing of information, which will enhance cooperation and coordination among member states in the area of ICT security. The proposed platform is intended to be a reference portal for member states who seek information related to ICT security, including on capacity-building and assistance programs.[10] While there have been discussions about whether such an initiative would lead to duplication of efforts given existing cooperation portals such as the GFCE cyber portal, the Indian proposal for GCSCP aims to combine all relevant sub-portals for small and developing countries to have easy access to multiple platforms and track different portals.

C. Mapping International and Regional level Cyber Capacity-Building Initiatives

ASEAN Institute for Peace & Reconciliation (ASEAN-IPR)[11]

The ASEAN-IPR is mandated to be an ASEAN institution for research activities on peace and conflict management. In a programme funded by the ASEAN – Korea Cooperation Fund (AKCF),[12] to address a wider ambit of peace-building through a comprehensive approach, the ASEAN-IPR undertook a youth capacity-building workshop for youth to utilise technology as an instrument of peace. The workshop was convened virtually in September 2021[13] and designed around the key theme of "Youth and Digital Technology for Peace" and was attended by representatives from ASEAN Member States, Republic of Korea Mission to ASEAN, ASEAN-

Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/A-AC.292-2023-1_Secretariat_Background_Paper_PoC_[Advanced,_unedited_English_version]_2.pdf>

[9] Working Paper on Global Cyber Security Co-operation Portal, Permanent Mission of India to OEWG <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/A-AC.292-2023-1_Secretariat_Background_Paper_PoC_[Advanced,_unedited_English_version]_2.pdf>

[10] Working Paper on Global Cyber Security Co-operation Portal, Permanent Mission of India to OEWG <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/A-AC.292-2023-1_Secretariat_Background_Paper_PoC_[Advanced,_unedited_English_version]_2.pdf>

[11] 'Asean-IPR Training & Capacity Building Programme' (*AKCF - ASEAN Korea Cooperation Fund*) <https://www.aseanrokfund.com/our-works/projectasean-ipr-training-capacity-building-programme>

[12] (*AKCF - ASEAN Korea Cooperation Fund*) <https://www.aseanrokfund.com/>

[13] 'ASEAN-IPR Training & Capacity Building Programme Youth and Technology Workshop' (*AKCF - ASEAN Korea Cooperation Fund*) <https://www.aseanrokfund.com/news/asean-ipr-training-capacity-building-programme-youth-and-technology-workshop>

IPR, ASEAN Secretariat, and youth across the region. To enhance the participants' engagement on the topics under discussion, the workshop organised various interactive activities to enable youth participants to make decisions based on different hypothetical scenarios related to the youth's experience on the digital platforms.

Asia-Pacific Cybercrime Capacity-Building Hub (APC_HUB)

The APC-HUB is a capacity-building training institution that provides training on combating cybercrime to lawmakers, policymakers, judges, prosecutors, investigators, and all other multi-stakeholders in the Asia-Pacific region.[14] The APC HUB undertakes training introduction and education related to cyber capacity-building efforts. APC-HUB's education and training aims to provide training not only on laws and policies related to cybercrime, but also criminal procedures, analysis techniques, and latest trends in investigation, analysis, and trial in a customised manner for each country's situation.[15]

ASEAN Cyber Capacity Programme (ACCP)

The ACCP is funded by Singapore and was initiated in 2016 with the purpose to support various efforts to improve cyber capacities across ASEAN member states.[16] Focus areas under the programme include cyber policy, legislation, strategy development as well as incident response. In the framework of this program, a physical ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) was established in 2019 under the aegis of the Cybersecurity Agency of Singapore.[17] The ASCCE conducts research and provides training related to cyber strategy and policy, international law and norms and legislation; provides CERT-related technical training; and conducts virtual cyber defence trainings and exercises.[18] Together with ASEAN Dialogue Partners, other international partners from governments, NGOs, private sectors and academia,

[14] About APC-HUB <https://www.apc-hub.org/>
[15] Capacity Building (*APC-HUB*) <https://www.apc-hub.org/capacity-building>
[16] Factsheet on ASEAN Cyber Capacity Programme <https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0>
[17] *ASEAN-Singapore Cybersecurity Centre of Excellence* <https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence>
[18] *'Asean Cyber Capacity Programme (ACCP)' (Cybil) <https://cybilportal.org/projects/asean-cyber-capacity-programme-accp/>*

ACCP along with the ASCCE have conducted more than 30 programmes to date.[19] The latter has reached over 900 senior government officials from ASEAN and beyond.[20]

ASEAN Regional Forum (ARF)

The ARF established the Points of Contact Directory on Security of and in the Use of Information and Communications Technologies in 2020.[21] The directory comprises national contact points for both senior level and working level contacts. If an ARF Participant has a central agency or body nominated by their government to coordinate the nation's conflict prevention, crisis management and response in relation to the security of and in the use of ICTs, a point of contact is established within this body to serve as the single point of contact for all ICT security incidents of regional significance.[22]

Cybersecurity Capacity Centre for Southern Africa (C3SA)[23]

Research ICT Africa has partnered with the University of Cape Town (UCT), the Global Cyber Security Capacity Centre, Oxford Martin School, the Department of Computer Science, University of Oxford and the Norwegian Institute of International Affairs (NUPI) in launching the Cybersecurity Capacity Centre for Southern Africa.[24] C3SA aims to provide a single-entry point for cybersecurity capacity building and research activities in the Southern Africa region and beyond. The centre will serve as a coordination and collaboration hub between cybersecurity capacity-building actors in order to reduce duplication of efforts on cyber capacity-building in the region.[25] C3SA's aims are to strengthen the African region's competence to fight cybercrime, promote women's participation in cybersecurity research and policymaking, increase the scale,

[19] Ibid
[20] *'Asean Cyber Capacity Programme (ACCP)' (Cybil) <https://cybilportal.org/projects/asean-cyber-capacity-programme-accp/>*
[21] Joint Working Paper by Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, the Republic of Korea, Mexico, the Netherlands, Singapore and Uruguay (*Implementing cyber confidence measures globally -towards the UN Point of Contact Directory)* <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Joint_Working_Paper_-_Next_steps_to_a_UN_PoC_Directory.pdf>
[22] Ibid
[23] Research ICT Africa, 'Cyber Capacity Centre for Southern Africa' (*Research ICT Africa*, 29 December 2022) <https://researchictafrica.net/project/cyber-capacity-center-for-southern-africa/>
[24] Ibid
[25] 'C3SA Home: University of Cape Town' (*C3SA Home | University of Cape Town*) <https://c3sa.uct.ac.za/#:~:text=C3SA%20is%20hosted%20by%20the,capacity%20building%20in%20the%20region.>

pace, and quality of cybersecurity capacity-building, and contribute to an open, free, and resilient Internet.

India - UK Counter Ransomware Initiative

India's National Security Council Secretariat (NSCS) and the UK Government in collaboration with British Aerospace Systems, successfully designed and conducted a counter-ransomware programme for 26 countries in May 2022 as part of the International Counter Ransomware Initiative- Resilience Working Group.[26] The programme was led and designed by India's National Cyber Security Coordinator (NCSC) to participate in a virtual ransomware drill and test their capabilities to share threat information and respond to ransomware incidents efficiently.[27] The programme involved discussions on methodologies to counter ransomware, important ransomware incidents in the past and experiences for predictive analysis, government's involvement and role in managing ransomware incident response, and how to incentivise the reporting of ransomware incidents, among other related issues.[28]

India's Counter Ransomware Seminar for Shanghai Cooperation Organisation (SCO)

The National Security Council Secretariat (NSCS), in association with the Data Security Council of India (DSCI) organised a two-day seminar in December 2022 for delegates of the Shanghai Cooperation Organisation's (SCO) member states.[29] India conducted this seminar on assuming the chairmanship of the Council of Regional Anti-Terrorist Structure under the SCO (RATS SCO) in October 2022. The seminar on "Securing Cyberspace in the Contemporary Threat Environment" focused on the changing nature of online crime and criminal behaviour in order to understand the threats, trends, issues, responses and ethical questions associated with the use of technology, by terrorists, specifically. The program also examined issues related to the cyber-

[26] 'India's NSCS & UK Govt in Collaboration with BAE Systems Successfully Designed & Conducted Cyber Security Exercise for 26 Countries' <https://newsonair.gov.in/News?title=India%E2%80%99s-NSCS-%26-UK-Govt-in-collaboration-with-BAE-Systems-successfully-designed-%26-conducted-Cyber-Security-Exercise-for-26-Countries&id=447235>
[27] 'India & UK Conducts Counter Ransomware Exercise for 26 Nations' (*Press Information Bureau*) <https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1857243>
[28] International Cooperation *(Indian Cybercrime Coordination Centre*) <https://i4c.mha.gov.in/who.aspx>
[29] 'India Organises SCO Meet to Brainstorm Emerging Threats in Cyberspace' (*The Economic Times*) <https://economictimes.indiatimes.com/news/defence/india-organises-sco-meet-to-brainstorm-emerging-threats-in-cyberspace/articleshow/88214160.cms>

realm from an interdisciplinary and multi-dimensional perspective to uncover different ways to approach current challenges.[30]

Cyber BRICS Project

The Cyber BRICS project aims to map existing regulations, identify best practices and develop policy suggestions in the areas of cybersecurity and personal data regulations, Internet access policies, and digital transformation strategies in the BRICS (Brazil, Russia, India, China and South Africa). The project is hosted by Fundação Getulio Vargas (FGV) Law School and developed in partnership with the Higher School of Economics, in Moscow, Russia; the Centre for Internet and Society, New Delhi, India; the Fudan University, Shanghai, and the Hong Kong University, China; and the University of Cape Town, Cape Town, South Africa.[31] The Cyber BRICS project facilitates research on key issues of cyber and digital governance, such as the development of a comparative interactive platform to examine connectivity across BRIC countries[32] and the examination of interoperability to foster Open Digital Ecosystems in the BRIC countries.[33]

India-EU Cyber Dialogue

In the context of the strategic partnership between India and the EU,[34] a cyber dialogue mechanism has been established to provide a platform for both Indian and EU representatives to discuss a wide range of issues related to cyberspace, cyber policies, strategies and areas of mutual interest. Both India and the EU have committed to joint efforts to promote an open, free, stable and secure cyberspace and increase cooperation on cyber security, as well as combat and prevent cybercrime through the promotion of existing international standards and norms in their respective areas. The most recent 7th cyber dialogue[35] involved discussions on cyber cooperation in multilateral fora and in regional settings such as the OSCE, ARF and G20. They also discussed

[30] 'Rats SCO Practical Seminar on Securing Cyberspace in the Contemporary Threat Environment, December 2021' (*Press Information Bureau*) <https://pib.gov.in/PressReleasePage.aspx?PRID=1779848>
[31] About Us *(CyberBRICS)* <https://cyberbrics.info/>
[32] 'Connectivity across BRICS Countries' (*CyberBRICS*, 21 August 2023) <https://cyberbrics.info/connectivity-across-brics-countries/>
[33] Demambro J, 'Interoperability to Foster Open Digital Ecosystems in the BRICS Countries' (*CyberBRICS*, 23 August 2023) <https://cyberbrics.info/interoperability-to-fosteropen-digital-ecosystems-inthe-brics-countries/>
[34] 'India Strategic Partnership: A Roadmap to 2025' (*EU*) <https://www.eeas.europa.eu/eeas/eu-india-strategic-partnership-roadmap-2025_en>
[35] Ministry of External Affairs, India (*Seventh India-EU Cyber Dialogue)* <https://www.mea.gov.in/press-releases.htm?dtl/37162/Seventh+IndiaEU+Cyber+Dialogue>

cooperation in promoting capacity-building in cyberspace and combating the criminal use of ICTs.

Organization of American States (OAS)

The Organization of American States' (OAS) Working Group on "Co-operation and Confidence Building Measures in Cyberspace" undertook the identification of national Points of Contacts (PoCs) at the political level to discuss the implications of hemispheric cyber threats in 2018.[36] The working group has also designated PoCs in Ministries of Foreign Affairs of member states to strengthen cooperation on cyber diplomacy and to facilitate international dialogue.[37] The OAS Confidence Building Measure portal allows members of the working group to access the list of PoCs and contact any registered PoC.[38]

D. Key Takeaways & Insights

The organisations, forums and initiatives mapped above do not represent an exhaustive list of cyber capacity-building initiatives at the national and regional levels outside of the United Nations. This mapping exercise was carried out to highlight the different organisational ways in which capacity-building is being approached, particularly from the perspective of developing countries. The following are key takeaways from the initiatives highlighted above as well as broader recommendations to guide the OEWG's approach to cyber capacity-building initiatives:

- The establishment of more cyber coordination centres like the Cybersecurity Capacity Centre for Southern Africa, to build diverse consortiums of research organisations, universities and technical entities from across the world, can help reduce the duplication of efforts at regional levels for cyber capacity-building initiatives.

[36]Organisation of American States, *Confidence Building Measures in Cyberspace* <https://www.oas.org/en/sms/cicte/Documents/2016/Speeches/JAMES%20LEWIS%20CSIS.pdf>
[37]Organisation of American States, *Confidence Building Measures in Cyberspace* <https://www.oas.org/en/sms/cicte/Documents/2016/Speeches/JAMES%20LEWIS%20CSIS.pdf>
[38] Confidence building measures in cyberspace *(Organization of American States)* <https://www.oas.org/en/sms/cicte/Documents/2016/Speeches/JAMES%20LEWIS%20CSIS.pdf>

- The ASEAN Cyber Capacity Programme is a good example of how countries can prioritise resources and leverage existing cybersecurity institutions at the national level to promote capacity-building initiatives at the regional level.

- The ASEAN Institute for Peace & Reconciliation's workshop on engaging with the youth for digital best practices is a good example of how cyber capacity initiatives can be built into programmes with broader global stability and peace agendas. The OEWG can compile a list of organisations, platforms and forums with broader agendas that align with its normative framework goals, under which cyber capacity-building activities can be introduced.

- ASEAN plays an important role in cyber capacity-building initiatives in the Asia Pacific region. The range and number of cyber programmes and initiatives being driven by ASEAN is a positive sign for the improvement of cyber growth and resilience at all levels. The regional initiatives undertaken by ASEAN can further be analysed to evaluate the impact that various capacity-building initiatives have on the overall security and resilience of ICT capabilities of these countries. This can help countries determine which of the existing initiatives are best suited to their cybersecurity development needs. Other regional organisations such as the South Asian Association for Regional Cooperation, African Union, Shanghai Cooperation Organisation, etc., can also benefit from such impact insights to find ways in which their contribution or collaboration can help widen the reach of cyber capacity initiatives at regional levels.

- The establishment of bilateral agreements and initiatives should be leveraged by developing countries amidst the growing strategic importance of cyberspace and digital cooperation in such agreements. For instance, India has established joint declarations and/ or memorandums of understanding with countries including Bangladesh, Bulgaria, Estonia, Israel, Japan, South Korea, Singapore, EU, France, Germany and the United Kingdom.[39] Such cooperative efforts can help countries tailor the exchange of cyber knowledge, capacity and information to their respective priority areas and needs

[39]Sukanya Thapliyal, 'Analysing India's Bilateral Mous in the Field of Information and Communication Technologies (Icts)' (*The CCG Blog*, 11 May 2022) <https://ccgnludelhi.wordpress.com/2022/05/11/analysing-indias-bilateral-mous-in-the-field-of-information-and-communication-technologies-icts/>

benefiting both parties.

- The OEWG's Final Substantive Report (2021) established the importance of capacity building initiatives to "respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory".[40] Gender sensitive approaches[41] to cyber capacity-building initiatives should be prioritised in the development, implementation and evaluation of regional and national programmes. This will help ensure meaningful inclusion of women and LGBTQIA+ people and in the development of the global cybersecurity ecosystem.

- Capacity-building initiatives that are designed for developing countries should adopt a whole-of-government approach[42] that recognises the presence of extensive processes, mechanisms and collaboration across all levels of government for strengthening the cybersecurity ecosystem at the national level. The principle of "common but differentiated responsibility" can be used to operationalise such an approach and ensure that the responsibility for a country's cybersecurity is taken into consideration by different levels and departments of government.[43]

[40] A/AC.290/2021/CRP.2, Final Substantive Report, Open-ended working group on developments in the field of information and telecommunications in the context of international security, 10 March 2021, United Nations General Assembly <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf> f
[41] Association for Progressive Communications, A Framework for Developing Gender-Responsive Cybersecurity Policy Norms, Standards and Guidelines <https://www.apc.org/sites/default/files/gender-cybersecurity-policy-norms.pdf>
[42] Centre for Communication Governance, Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2022 <https://drive.google.com/file/d/14XfyXu-5sAPgzAmEaKE78vphTTfH_Y5s/view>
[43] Gunjan Chawla, Ananya Moncourt and Vagisha Srivastava, Working Paper: The Cybersecurity Budget Brief, Centre for Communication Governance, National Law University Delhi_ January 2023. <https://drive.google.com/file/d/1_YMPhBhiq2guJlW2Zhej6Wo8ftEhMjps/view>